International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-1, November 2019

Secure Data Performance Analysis with OLSR and AODV Routing Protocols in MANET

S. Ismail Kalilulah, B. Justus Rabi, Vidhya V

Abstract – MANETs are vigorous network to obligate node links due to the wireless frequency affect the network performance. It evaluates the link constancy by redefining the link availability that connected throughout a specific time period. MANETs have an identical status to acquaintance by the node resources with any other network. In this work, network is able to deal with vital reform that competent, consistent, and accessible network to perform enhance network protocol along with data security. AODV network nodes need connections broadcast forward the message that requested a connection that create a series of impermanent routes back to the requesting node. In this work, a link state protocol is calculated an alternative and fragmented path from source to destination by re-routing traffic through it, regardless of the locations of failure and the number of failed links. Also, the purpose of this research work is to provide secure bit data networking and occupy bit-memory address to enhance the node data capacity size, hence it reduces packets loss, delay time, and improve throughput when re-join the nodes while failure. OLSR generate a control overhead to maintain routing table to consume data traffic bandwidth. This study reduces the control overhead to improve the performance of OLSR by optimizing control messages intervals to have enhanced and secure data transmission. In this work, a secure and reliable bit-data is presented which have a memory address search process between two data address as simulated in this work.

Keywords – AODV, MANET, OLSR, Routing Protocols, Intervals

I. INTRODUCTION

MANET has the wireless frequencies without a fixed network communication and consolidated direction. The wireless nodes routers are transformed network frequently can endure data communication link which is asymmetrical between the nodes. The network design features of the transmitter and receiver are depending on the link transmission that includes;

(i) Node data receives from another node which is unable to transmit due to the asymmetric links.
(ii) The nodes communicate with each other using local transmission with a symmetric link.

The node data broadcasts the route discovery over the network while a routing request is being dispensed and forwards the route data to improve address into the source inclination. The advantages of the MANET routing protocol is an efficient route creation between a couples of nodes with a slightest of overhead and bandwidth consumption.

Revised Manuscript Received on November 30, 2019.

***** Correspondence Author

Dr. S. Ismail Kalilulah*, Assistant Professor, Department of CSE, Dr. M.G.R. Educational and Research Institute, Chennai, India. E-Mail: ismailkalilulah125@gmail.com

Dr. B. Justus Rabi, Department of Electrical and Electronics Engineering, M. S. University, Tamil Nadu, India. E-mail: bennisrobi@rediffmail.com

Ms. Vidhya V, Assistant Professor, Dr. M.G.R. Educational and Research Institute, Chennai, India. E-mail: vidhyaaug7@gmail.com

The disadvantage is that the protocol performance is not sufficient as it needs pause time and QoS improvements to get consequences for effective data transmission.

1.1 MANET Performance in a Secure Wireless Communication

MANET is a cluster of wireless nodes emergent a network without the use of any established network infrastructure. MANET compresses with nodes to perform wireless communication. The wireless nodes forward communication radio arrays to the nodes in a

peer-to-peer network environment. MANET nodes are able to distinguish the occurrence of other nodes and perform the essential set-up to enable communications

to share data and network services. The categories of MANET have an independent routing process for competent, robust and secure network are included,

(i) *Distributed Data Operation*: Control and manage the distributed network.
(ii) *Independent Node Terminal*: Functions as a host and a router that typically distinguish both endpoints and switches in network.
(iii) *Multihop routing*: Link layer attributes and routing protocols are based on a hop that is reluctant than multihop structure.
(iv) *Light-weight Node Systems*: Compute and communicate the functions with irrelevant memory size, and squat power storage.
(v) *Mutable Link Capacity*: Node stations interconnect to noise that vanishing and interference with less bandwidth in network.
(vi) *Vibrant Network System*: Node terminals vary time measurements to adapt the network traffic and broadcast.

1.2 AODV Routing Protocol in MANET

AODV is a routing protocol designed to establish routes to destinations on request and supports the multicast routing that does not create further traffic for communication node links. Adhoc network converses with multi-hop wireless links where each node acts as a router in the network. The routing protocol growth finds routes among communication nodes that modify the network topology. MANET cluster of nodes interchange data arbitrarily where each node acts as a host and a router forwards and receives data packets in the network. The node transmission range of the network realise other nodes vigorously. MANET features are having vigorous topology, inadequate corporal security, node energy constrained nodes and controlled bandwidth links to provide multi-hop routing rather than a stagnant infrastructure based network. AODV minimizes the routing overhead that enhances the performance of the network such as average end-to-end delay, throughput and packet delivery ratio. It includes limited desirable bandwidth include the following are,

(i) Minimize the routing protocol space complexity.
(ii) Maximize the utilization of the network bandwidth.
(iii) Each source node should initiate unique path discovery process.
(iv) Maintain loop-free routes by using the logic of nodes to remove node packet broadcast identity.

II. LITERATURE SURVEY

Abolhasan M., et al., [2004] presented MANET performance efficiency of the routing protocols that adapt frequent changes in network topology and link status. Asma et al., [2015] proposed a control message AODV routing protocol to improved network route. Chen Y., at al., [2002] presented the routing protocols to find a single route between nodes accomplishing the QoS. Geetika et al., [2016] proposed a dependence estimator node to evaluation neighboring nodes. Harsimran and Jasvir [2017] presented provides comparison between AODV and DSDV protocol. Joshi, et al., [2012] proposed a route transfer between different nodes using OSPF to varying the physical and logical circumstances of networks. Karamjeet, et al., [2012] proposed a traffic data transmission, bit error rate/packet, throughput to represent a propoer route in network. Kurkowski, et al., [2005] proposed the performance analysis of wireless protocols in the context of MANETs. Lakshman, et al., [2018] proposed the QoS to analysed the OLSR improve its performance. Md. Niaz, et al., [2015] proposed the performance evaluation of routing protocols that consider mobility factor to reveal better performance in OLSR. Me´rindol, et al., [2010] presented the K-SPF algorithm and calculate various paths. Mounir, et al., [2002] proposed the secure network performance metrics to vary the control messages intervals to reduce control overhead. Mueen Uddin, et al., [2012] presented on demand routing algorithm to perform better than other outdated algorithms. Navaid, et al., [2012] presented the outperform execution to decrease the routing overhead without any additional extra cost. Perkins and Royer [1999] presented AODV routing protocol usages a broadcast route discovery mechanism depends on route establishment. Preeti and Pabitra [2011] proposed a method to secure AODV routing protocol to avert the attacks that vary routing data. Radwan S., et al., [2011] presented a reroute traffic via an alternative path whose local link wait until the source node is recognizes about the failure. Renuka, et al., [2017] proposed a mesh network which is based on different parameters in MANET. Selladevi and Duraisamy [2018] proposed a solution to detect and prevent attacks to transfer secure data. Yufei [2014] presented the analysis of fine tuning routing attributes to test different traffic transactions in the MANETs. Yu-Doo et al., [2009] proposed to improved routing protocol using AODV to analyse the network. Zhang, et al., [2009] proposed a node router maintain a routing table to have awareness of network nodes. Zuhi and Satish [2018] presented the routing protocols and cryptographic algorithms contract with a definite attack in network.

III. OLSR ROUTING PROTOCOL FOR DATA OVERFLOW PROCESS

MANETs are having OLSR protocol that does not manage routing process and provides the routing information to all distribution network hosts. OLSR protocol mechanism optimizes overflowing control protocol to build and endure routing tables by diffusing fractional link state information to network nodes. OLSR protocol benefits and drawbacks are given in Table 1.

Table 1 OLSR protocol benefits and drawbacks

Benefits	Drawbacks
• Lower route discovery latency on-demand protocols due to its preemptive environment. • Increase the frequency contention leads network congestion that reduces the wireless network performance.	• Host sends updated data by overflowing in OLSR protocol while network data transmission. • OLSR generates a control overhead to consume treasurable bandwidth in network process.

The node link state procedure is complicated in network and each router has its specific network map. The node routing tables are built through the process of the protocol switching routing to update node packets. MANETs have an OLSR routing protocol with an operative apparatus link state packet forwards to optimize various methods and informs the comprehensive advanced proficiency that includes,

(i) Moderate the control packet sizes and reduce the links to dispatch the link state packets.
(ii) Link state size reduces by a detachment of node links where the subsets are the neighbors of every node and selected to transmit link state updates.
(iii) Periodic link state modernizes in the process of optimization that does not produce additional control packets.

The node transmission rate is equivalent to the number of nodes as shown in Figure 1 as OLSR node data overflow process. In OLSR, each node chooses node sets to execute the processing and forwarding of link state packets in the network.

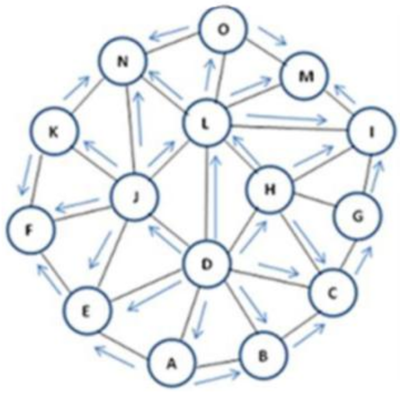


Fig. 1 OLSR node data overflow process

3.1 Node Route Location Procedure with CBRP Approach

The node route location approach is using the cluster-based routing approach (CBRP) which has various clusterheads to choose a routing process. The clusterhead process is able to communicate with each other by using gateway nodes that performed as source routing by saturating the network with a route request communication. This procedure stores neighbouring data clusters as shown in Figure 2 where the data clusters A,B and A,C are bi-directionally linked, clusters C,D are unidirectional linkage.

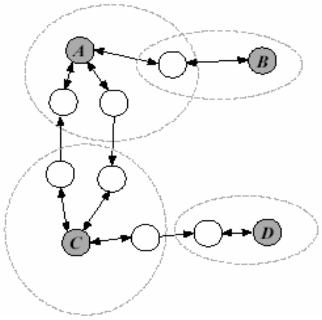


Fig. 2 Node link connectivity between data clusters

The node route location method usages the source routing where the cluster heads are drowned with node route request array (NRRA**)**. The access nodes receive the NRRAs without broadcasting the route method and forward to the next clusterhead. This strategy moderates the network traffic broadcasts with NRRA that have uniqueness to the access nodes and reach to the cluster address. A clusterhead receives NRAA to compute a source route consists to form a shortest path within each cluster as shown in Figure 3.

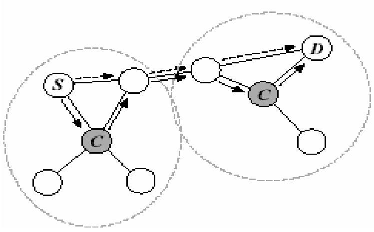


Fig. 3 Movable source route (un-dashed arrows) and the strict source route

3.2 OLSR Packet Control Droplets

The node detection link failures exchange data information needs to handle node packets dropped by OLSR that store the packet in a buffer queue process. Each packet is stored in the queue process, current value of the copy_count parameter and the opp_TTL value is time based parameter indicates the local time to remove mode packet queue process. The end of the node packet control droplet protocol returns to typical OLSR operation as shown in Figure 4.

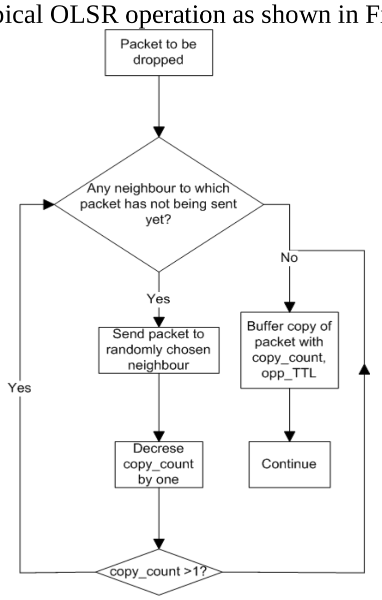


Fig. 4 Handling node packet drops in queue process

IV. NODE LINK NETWORK CONNECTIVITY WITH CONSTRUCTIVE MODEL

A node probabilistic model describes an associate link which is based on metrics to evaluate the link stability is defined. Let, *a* and *b* signify random nodes in the network, send a packet from node *i* to node *j* at a random time instant *t* can be effectively received by node *b* that follows node signal condition is as given in eqn. [1],

$$\frac{NP_i(t) f_{ab}(t)}{N_b + \sum_{k \epsilon I_a(t), k \neq a} NP_k(t) g_{kb}(t)} \geq \delta_b \qquad \ldots (1)$$

where, N_b represents the contextual signal at the receiver of node *b*, NP_i *(t)* symbolizes the transmitting power of node a, $f_{ab}(t)$ is the frequency enhancement from node *a* to node *b*, $I_a(t)$ interfere node transmission where time instant *t*, and δ_a is the node signal requirement for the receiver of node *b* to translate a node packet. The link from node $a \rightarrow b$ is connected at time *t* while eqn. [1] is satisfied. If the two wireless frequency nodes are identical then link $a \rightarrow b$ can be considered as bi-directional link node. The wireless frequency arbitrary property has the connectivity of link *a* ↔ *b* can be signified by the process as given in eqn. [2],

$$W_{ab}(t) = \begin{cases} 0, & \text{Link } a \leftrightarrow b \text{ is not linked at time } t \\ 1, & \text{Link } a \leftrightarrow b \text{ is linked at time } t \end{cases} \qquad \ldots (2)$$

The wireless frequency presence $W_{ab}(t)$ has wireless node link connectivity which is stable at low swiftness transmission. The node packet function is designated by the error probability to confirm the node packet end-user efficiently. The node link interval connectivity (*NLIC*) sequence model is link *a* ↔ *b* where transition rate from *state* 0 to *state* 1 is represented by $\varphi_{ab}(t)$, and the transition rate from *state* 1 to *state* 0 is represented by $\alpha_{ab}(t)$. The subsequent arbitrary series $\{W_{ab}(k\Delta t)\}$ is regarded as the yield of discrete-time link connectivity prototypical for link *a* ↔ *b*. At this time, the subscripts *a* and *b* are vanished where no indistinctness occurs within a definite interval, $\varphi(t), \alpha_{ab}$ and $q_{ij}(t)$ are independent of *t*, denoted by φ, α and q_{ij} respectively. By an arbitrary sample the output W_{ab} (t) of the NLIC obtain the transition matrix as given in eqn. [3],

$$NP(\Delta t) = \frac{1}{\lambda + \alpha} \begin{bmatrix} \alpha + \lambda r^{-(\lambda+\alpha)\Delta t} & \lambda + \lambda r^{-(\lambda+\alpha)\Delta t} \\ \alpha + \alpha r^{-(\lambda+\alpha)\Delta t} & \lambda + \alpha r^{-(\lambda+\alpha)\Delta t} \end{bmatrix} \qquad \ldots (3)$$

In eqn. [3], the estimation viewpoint link states based on the transition chances at present time, as long as the time estimation lies in the equivalent interval as the obtainable time.

4.1 Node Link Constancy Metrics for Data Transitions

The node link stability metrics initiate with the finite conditions is dependable when its transition rates are constant over separated intervals but time alliance does not constant. A chain with *K* conditions, let $qi'j'(t)$ represent a transition rate from state *i*′ to state *j*′ (*i*′, *j*′ = 0, 1,…, *K*-1) and separate particulars on the time axis where waiting time of a conditional transition has an exponential distribution have $\aleph_{01}$ represent waiting time and $\aleph_{10}$ represent waiting time for both *state* 1 to *state* 0 transition. A definite consistent time interval is given in eqn. [4],

$$\begin{cases} NP\{\aleph_{01} > \sigma\} = r^{-\lambda\sigma} \\ NP\{\aleph_{10} > \sigma\} = r^{-\alpha\sigma} \end{cases} \quad \ldots (4)$$

where, $\sigma \geq 0$. Let, the present time t_q evaluate the node link stability possibility that remains link connected for time τ probability as given in eqn. [5],

$$q_{persist}\ (\sigma) = NP\{\aleph_{10} > \sigma) = r^{-\alpha(t_q)\sigma} \quad \ldots (5)$$

where, the prospect of the link recovers within time σ after a link failure as given in eqn. [6],

$$p_{recuperate}\ (\tau) = NP\{\aleph_{01} \leq \sigma) = 1 - r^{-\lambda(t_q)\sigma} \quad \ldots (6)$$

The node link remains associated probability for a specified time σ estimate the node link connectivity represents $q_{persist}\ (\sigma)$ is a significant than $p_{recuperate}\ (\sigma)$ can be implemented to normalize whether a link failure is progressive while data communication.

4.2 Data Transition Rate Evaluation in Link Constancy

The link constancy chore evaluations the possibilities with different values of σ are estimated to consider the link state illustrations from the consistent interval in the NLIC and appraise $q_{persist}(\sigma)$ and $p_{recuperate}(\sigma)$ accordingly. The node link network interval has an exponential distribution to calculate φ and α with the joint value of the mean time of a link where the connected network time is condensed and increase estimation errors. The estimation of q_{ij} for data transition evaluates the occurrence of the nodes within its transmission range. The time interval of Δt obtain the connectivity of link $a \leftrightarrow b$ based on node a has acknowledged from node b at each sampling instantaneous. Therefore, the transition of q_{ij} is evaluated based on the link state models where the matrix of transition probability is expressed as eqn. [7],

$$NP = \begin{bmatrix} q_{00} & q_{01} \\ q_{10} & q_{11} \end{bmatrix} \quad \ldots (7)$$

where, $q_{i0} + p_{i1} = 1$. Let us have,

$$X_i = \begin{cases} 0, & W_{k+1} \neq W_k \\ 1, & W_{k+1} = W_k \end{cases}, for\ \forall k \epsilon Y, W_k = i \quad \ldots (8)$$

where, $W_k = W\ (k\Delta t)$ and $\boldsymbol{Y}$ is the set of numerals. The probability function of X_i is,

$$f(x;\ q_{ij}) = q_{ij}^{x}(1 - q_{ij})^{1-x} \quad \ldots (9)$$

V. NETWORK SPEED CONTROL VARIATIONS PERFORMANCES

In this section, the effects of network size and mobility speed variations are based on the throughput performance. The network sizes with 5, 20 and 30 nodes and two mobility speeds of 10 m/s and 20 m/s are used to analyse the delay performances in each protocol, where it shows the collisions occurrences at different node points.

5.1 AODV based secure network throughput analysis

Figure 5 indicates the effects of network size and mobility speed variations on the throughput performances of AODV, where node speed variations perform with a secure data encryption standard (DES) mechanism with an appropriate and rapid path to the network.

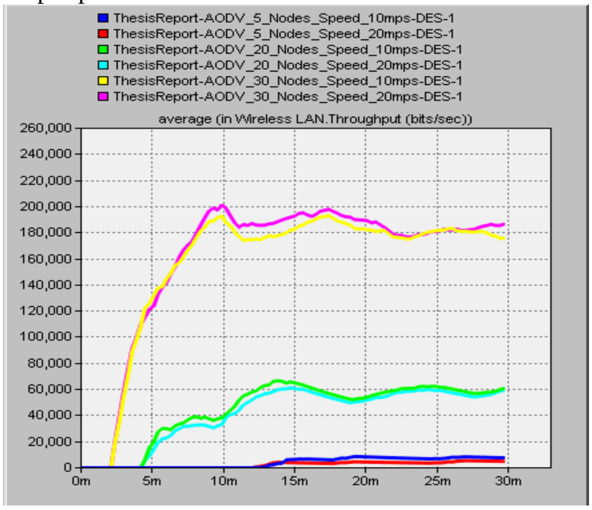


Fig. 5 Impact of network size and mobility speed on the throughput of AODV

It is experimented the graphical view to perform AODV the throughput that increase the number of nodes from 5 to 20 and then to 30. Hence, the network sizes measured the throughput which is better in larger network sizes and designates several nodes having redundant links and less link failures to reduce the node packet drops while transmission of node data.

5.2 Secure Network Throughput Analysis with OLSR Protocol

The influence of secure network size and transmission speed variations is on the OLSR throughput performance represented in graphical view in Figure 6 that increases the node throughput performance irrespective of the flexibility network speed variations. The highest OLSR throughput performance was observed 30 numbers of nodes trailed by the 20 nodes network size as follow the secure and hasty network path from one to another end-point to the network in data transmission.

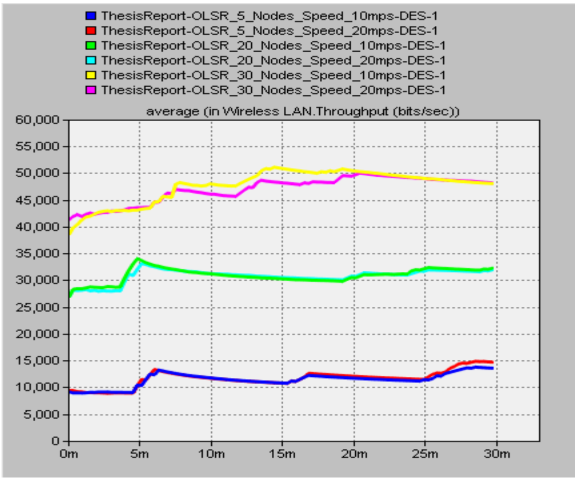


Fig. 6 Impact of network size and mobility speed on the throughput of OLSR

VI. RESULTS AND DISCUSSION

Figure 7 shows data address transmission from address1 to address2 which have 4 bits data respectively for OLSR and AODV routing protocol in MANET approach.

It shifts last bit from 0 to 1 to provide the strength security mechanism for secured data networking and occupy 64-bit (63:0) memory address to enhance the size of node data capacity in prospect MANET.

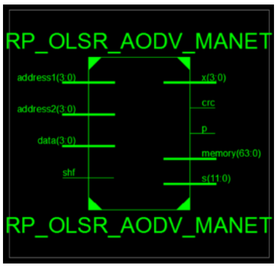


Fig. 7 Data address transmission with OLSR and AODV routing protocol in MANET approach

The adaptive routing model of each circuit generates the functions of routing protocol to perceive the behaviour of the network system as shown in Figure 8.

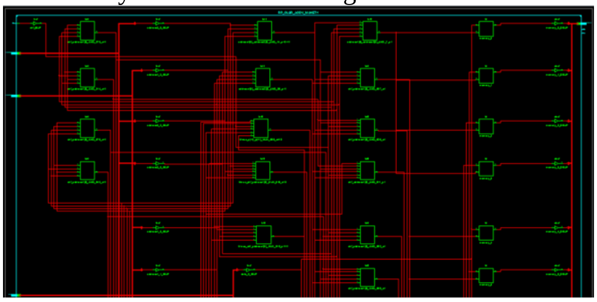
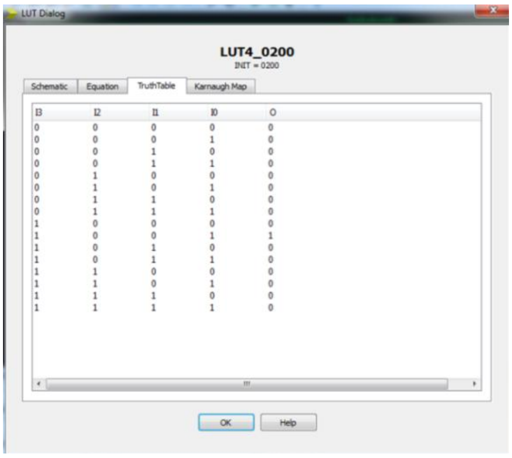


Fig. 8 Circuit generate function in routing protocol

In Figure 9, the hexa-decimal truth table is shown where karnaugh map (*k*-map) represent 1 at 1001, as error that could not provide an appropriate security to the node while data transmission.



I3	I2	I1	I0	O
0	0	0	0	0
0	0	0	1	0
0	0	1	0	0
0	0	1	1	0
0	1	0	0	0
0	1	0	1	0
0	1	1	0	0
0	1	1	1	0
1	0	0	0	0
1	0	0	1	1
1	0	1	0	0
1	0	1	1	0
1	1	0	0	0
1	1	0	1	0
1	1	1	0	0
1	1	1	1	0

Fig. 9 Hexa-decimal Truth table with *k*-map approach

The error is generated in k-map (green color) represent the error transpired block as shown in Figure 10.

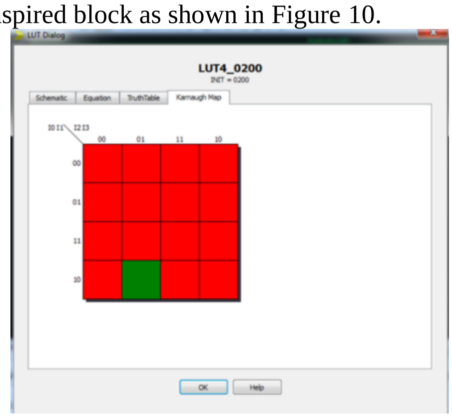


Fig. 10 Error transpired block in *k*-map

This work results demonstrate the address1 and address2, where address data is transferred, it searches in the memory address of 64-bits as 0101 that shows that data is matched in the data array whenever search process occurred in the MANET environment as shown in Figure 11.

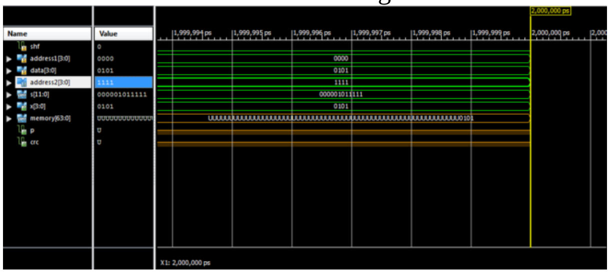


Fig. 11 Memory address search process between two data address

In our experimental work, when error occurred in truth table where delay occurred in data transmission because of error generated in data flow process as shown in Figure 12.

```
  Destination:        memory<3> (PAD)
  Source Clock:       address1[3]_address2[0]_AND_7_o falling

  Data Path: memory_3 to memory<3>
                                Gate     Net
    Cell:in->out      fanout   Delay   Delay  Logical Name (Net Name)
    ----------------------------------------  ------------
     LD:G->Q               1   0.323   0.339  memory_3 (memory_3)
     OBUF:I->O                 0.003          memory_3_OBUF (memory<3>)
    ----------------------------------------
    Total                      0.665ns (0.326ns logic, 0.339ns route)
                                       (49.0% logic, 51.0% route)

=========================================================================

Cross Clock Domains Report:
--------------------------

Clock to Setup on destination clock shf_address1[3]_MUX_616_o
-------------------------+---------+---------+---------+---------+
                         | Src:Rise| Src:Fall| Src:Rise| Src:Fall|
Source Clock             |Dest:Rise|Dest:Rise|Dest:Fall|Dest:Fall|
-------------------------+---------+---------+---------+---------+
shf_address1[3]_MUX_616_o|         |         |    0.746|         |
-------------------------+---------+---------+---------+---------+

=========================================================================
```

Fig. 12 Delay occurrence in data transmission rate in MANET approach

The practical experiment is developed and generated as output shows the error status where it represent the real-time transmission rate and accurate CPU consumption time as shown in Figure 13.

```
Cross Clock Domains Report:
--------------------------

Clock to Setup on destination clock shf_address1[3]_MUX_616_o
-------------------------+---------+---------+---------+---------+
                         | Src:Rise| Src:Fall| Src:Rise| Src:Fall|
Source Clock             |Dest:Rise|Dest:Rise|Dest:Fall|Dest:Fall|
-------------------------+---------+---------+---------+---------+
shf_address1[3]_MUX_616_o|         |         |    0.746|         |
-------------------------+---------+---------+---------+---------+

=========================================================================


Total REAL time to Xst completion: 28.00 secs
Total CPU time to Xst completion: 27.99 secs

-->

Total memory usage is 282996 kilobytes

Number of errors   :    0 (   0 filtered)
Number of warnings :  164 (   0 filtered)
Number of infos    :    1 (   0 filtered)
```

Fig. 13 Experimental setup with real-time transmission and CPU time consumption

VII. CONCLUSION

MANET is an independent system of mobile nodes connected by wireless links that perform towards the secure and efficient routing protocols. OLSR protocol is a preemptive protocol for low latency route determination in MANETs. In this work, OLSR designated enhanced network performance with a secure and encrypted bit data for routing protocol which is based on the influence of node mobility using various performance metrics.

This work results shows the optimization of OLSR control data that outperform the specific wireless node circumstances and analysis with realistic agility models to finalize protocol performance. In a wireless network, a link is present between two nodes, if both of them are within range of each other. Thus, in this case topology control boils down to controlling the transmitting ranges.

REFERENCES

1. Abolhasan M., T. Wysocki, and E. Dutkiewicz, "A review of routing protocols for mobile adhoc networks", Elsevier Journal of Ad Hoc Networks, 2004.
2. Asma Ahmed, A. Hanan, Izzeldin Osman, "AODV Routing Protocol Working Process", Journal of Convergence Information Technology, Vol. 10, No. 02, pp. 1-8, March 2015.
3. Chen Y., Y. Tseng, J. Sheu, and P. Kuo, "On-Demand, Link-State, Multipath QoS Routing in a Wireless Mobile Ad-Hoc Network", Proceedings of European Wireless, pp. 135-141, February 2002.
4. Geetika Sharma, Anupam Mittal, Ruchi Aggarwal, "Attacks on Ad hoc On-Demand Distance Vector Routing in MANET", International Research Journal of Engineering and Technology, Vol. 03, No. 06, June 2016.
5. Harsimran kaur, Jasvir Singh, "A Brief Review: Routing Protocols AODV and DSDV for MANET", International Journal of Advanced Research in Computer Science, Vol. 8, No. 5, pp. 630-635, May-June 2017.
6. Joshi S., Kurundkar S. and Waghmare L., "Performance Analysis of Routing Protocol with Mobility Constraint", IJCA Proceedings on International Conference and workshop on Emerging Trends in Technology, Vol. 7, pp. 13-16, 2012.
7. Karamjeet Kaur, Sukhjeet Singh, Rahul Malhotra, "Design of open shortest path first Protocol –a link state protocol using OPNET modular", Vol. 1, No. 1, pp. 21 – 31, December 2012.
8. Kurkowski S., T. Camp, and M. Colagrosso, "MANET Simulation Studies: The Incredibles", ACM SIGMOBILE Mobile Computing and Communications Review, pp. 50-61, October, 2005.
9. Lakshman Naik. L., R.U. Khan and R.B. Mishra, "MANETs: QoS and Investigations on Optimized Link State Routing Protocol", International Journal of Computer Network and Information Security, Vol. 10, pp. 26-37, 2018.
10. Md. Niaz Imtiaz, Md. Mohidul Hasan, Md. Imran Ali and Md. Mostak Shaikh, "Performance Evaluation of Routing Protocols (AODV, DSR, OLSR and DYMO) in MANET Considering Mobility Factor", International Journal of Scientific & Engineering Research, Vol. 6, No. 12, pp. 714-720, December 2015.
11. Me´rindol P., P. Francois, O. Bonaventure, S. Cateloin, and J.J. Pansiot, "An efficient algorithm to enable path diversity in link state routing networks", Computer Networks, 2010.
12. Mounir Benzaid, Pascale Minet, Khaldoun Al Agha, "Integrating fast mobility in the OLSR routing protocol", Mobile and Wireless Communication Networks, 2002.
13. Mueen Uddin, Azizah Abdul Rahman, Abdul Rahman Alarifi, Muhammad Talha, Asadullah Shah, Mohsin Iftikhar, "Improving Performance of Mobile Ad-Hoc Networks Using Efficient Tactical on Demand Distance Vector Routing Algorithm", International Journal of Innovative Computing, Information and Control, Vol. 8, No. 6, pp. 4375-4389, June 2012.
14. Navaid Akhter, Ammar Masood, Irfan Laone, "Performance Improvement of Optimized Link State Routing Protocol", Semantic Scholar, ICOMP'12, WorldComp, Las Vegas, Nevada, USA, 19th July 2012.
15. Perkins C.E. and Royer E.M., "Ad-hoc On-Demand Distance Vector Routing", Proceedings of the second IEEE Workshop o Mobile Computing Systems and Applications, New Orleans, L.A., pp. 90-100, 1999.
16. Preeti Sachan and Pabitra Mohan Khilar, "Securing AODV Routing Protocol in MANET Based on Cryptographic Authentication Mechanism", International Journal of Network Security and Its Applications, Vol. 3, No. 5, pp. 229-241, September 2011.
17. Radwan S. Abujassar and Mohammed Ghanbari, "Efficient Algorithms to Enhance Recovery Schema in Link State Protocols", International Journal of UbiComp, Vol. 2, No. 3, pp. 53-67, July 2011.
18. Renuka Sharma, Pankaj Kumar, Devottam Gaurav, "The Comprehensive Performance Evaluation of AODV and OSPF in WiMAX", International Journal of Computer Applications, Vol. 160, No. 6, pp. 29-36, February 2017.
19. Selladevi M., Duraisamy S., "Survey Paper on Various Security Attacks In Mobile Ad Hoc Network", International Journal of Computer Sciences and Engineering, Vol. 6, No. 1, pp. 156-160, 2018.
20. Yufei Cheng, "Performance Analysis of Transactional Traffic in Mobile Ad-hoc Networks", Department of Electrical Engineering & Computer Science, School of Engineering, University of Kansas, 2014.
21. Yu-Doo Kim, IL-Young Moon, Sung-Joon Cho, "A Comparison of Improved AODV Routing Protocol based on IEEE 802.11 and IEEE 802.15.4", Journal of Engineering Science and Technology, Vol. 4, No. 2, pp. 132 – 141, 2009.
22. Zhang L., H. Sun, Q. Sun, X.-Y. Hu and C. J. Guo, "Improvement of routing protocols AODV in wireless Ad-Hoc network", World Congress on Software Engineering, Hefei, China, 2009.
23. Zuhi Subedar, Satish Deshpande, "Hybrid Cryptography Approach for Securing MANETs – A Survey", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 6, No. 1, pp. 166-172, January 2018.

AUTHORS PROFILE

Dr.S. Ismail Kalilulah, is currently working as Assistant Professor CSE Department in Dr. M.G.R. Educational and Research Institute, Chennai. He obtained Ph.D. from St. Peter's Institute of Higher Education and Research in Computer Science and Engineering, Master's degree from Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology and Bachelor's degree from Dr. M.G.R. Educational and Research Institute Chennai he has published 4 papers in International and National Journals and 9 Conferences. His areas of interest include Cloud Computing, IOTS, Computer Networks Security, Programming Languages, Data Mining, Mobile Computing & AI and he has 9 years of teaching experience. he has attended and organized Seminar and workshops related to his area of research. He is a Life Member in IAENG and CSTA and Member in ISRD. EMail:ismailkalilulah125@gmail.com

Dr. B. Justus Rabi, assumed office as the Principal of Christian College of Engineering and Technology in the month of June 2019. Dr. Rabi is a multifaceted personality with multifarious interests in academics and social activities. He holds a bachelor's degree in Electrical and Electronics Engineering from M. S. University, a Masters from Madras University and a Ph.D. from Anna University. He has also acquired an MBA and a law degree, LLB.Dr. Rabi has a slew of publications in National and International journals of import. Most of his publications are Scopus / SCI indexed. He has produced a total of 10 Ph.Ds.' and is currently guiding 9 Ph.D. scholars. He has also guided M.Tech research dissertations. He has presented a raft of papers dealing in Power Quality Solutions, Intelligent Controllers, Data mining, Energy Conservation and technology management in both National and International Conferences. Email: bennisrobi@rediffmail.com

Ms. Vidhya V obtained her Masters in Computer Applications from Ethiraj college for women, Chennai affiliated to University of Madras. She has 5 years of teaching experience. She has guided several UG Projects. She is currently working as an Assistant Professor in Dr. M.G.R. Educational and Research Institute, Chennai. Email: vidhyaaug7@gmail.com