International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-4, November 2019

An Enhanced OLSR Protocol to Improve Performance Of UAV in Wireless Mesh Network

Jasleen Kaur, Om Prakash

Abstract*: Over the past few decades, wireless mesh network is the main area of research in small and large sized network structure. Wireless mesh network is a radio based network scheme that needs minimal structure and organisation. It has the capability to integrate the wired system and can be prolonged at minimum cost without losing the mobile nature. Routing protocols mainly affects the performance of the WMN. Some of the advantages of the WMN are cost effective, easy management, robust and reliable service. It is utilised in numerous application areas such as hospitality and healthcare applications, rescue actions and disaster controlling, broadband connection services at home and institutions. In WMN , some challenges faced are, unsuitable number of alternate routes among the pair of the hops, entire capacity decreased due to interference among the multiple connections, effect on security due to complex networks. In a wireless mesh network, described about the optimized link state routing protocol (OLSR) and works on network parameters. In routing protocol, an immediate routing is required so that the change in topology may lead to flooding of data to desirable hosts in the system. After that, routing, performance is evaluated with encryption method using DES. Data encryption standard (DES) is cryptographic method that is applied to block of information. In this research proposed work, developed a novel improved, optimised link state routing method to enhance the network performance end to delay, delivery rate and recover the loss of data from sender to receiver hop. Experimental analysis is done using various parameters metrices as end delay, packet delivery ratio and throughput. In this research, an improvement in discovery delay of PASER and FER is also increased. The frame error rate computed is based on the level ranges range from 0%, 10% and 20%. Moreover, packet delivery ratio is 70% and throughput is 81%.

Keywords* : Wireless mesh networks, Data encryption standard, Optimized link state routing, Multiple connections, Clients and routers.

I. INTRODUCTION

Wireless mesh network is created by numerous amounts of motionless wireless mesh routers. Such routers are interconnected wirelessly though mesh structure. Router's works as wireless access points for the clients (access points and personal computers) to connect to the system.

The client routers transfers and gets information through backbone system. More than one router is linked to a wired system as gateway node and fixed to the external system like as internet or more than one router. With the advent in technology, wireless system is an additional aspect in place of the wired system.

In the meantime, various developments. Wireless mesh networks (WMN) or the wireless mesh systems (WMS) are the recovering solution for the lowest price broadband internet access in the background of the innovative system. These networks connect to open connections with minimum price, simple deployment, and consistent service exposure. Wireless mesh network consists of mesh routers which have restricted mobility and compromises structure access to equally mesh and contracts users [3]. Wireless mesh networks considered fast method to select the mesh router as gateway hop. These are linked to the internet through wired connections. Routing is an essential approach in wireless as well as the wireless connections [4].

The structure of the wireless mesh networks consists of three different components of wireless systems.. The components are mesh gateway, mesh access points (mesh router) and mesh clients or the mobile hops. Clients are connected to mesh gateway through wireless or wired connections [5]. One mesh router data are relayed to other mesh access points, but few of the access points have extraability to work as gateway internet. Gateway routers regularly have the wired connections that communicate among mesh access points and internet [6].

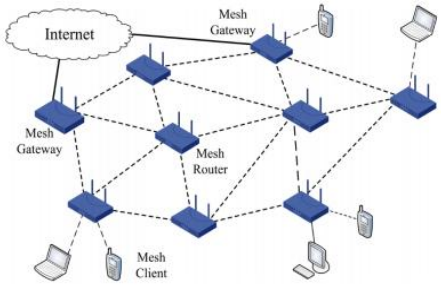

Fig 1. Architecture of Wireless Mesh Networks [5]

Manuscript published on November 30, 2019.
* Correspondence Author
Jasleen Kaur*, Department electronics and communication engineering, Shri JJT University, Rajisthan, India.
Om Prakash, department of electronics and communication engineering, MRIET, HYDERABAD, India,

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/

A. Advantages of Wireless mesh networks

Some of the advantages of wireless mesh network are self-arrangement, self- configuring , enables fast deployment of the nodes and better maintenance of the system [7]. WMN receives all the features of the generalised wireless ad hoc networks. Mesh routers are mainly immovable due to the motion of the ad hoc hopes. Some of the advantages are listed as;

- Cost effective technology.
- Self –configured
- Simple to design the structure
- Performs better more or less number of hops

B. Challenges of Wireless mesh networks

- Delay in attack detection due to multi-hop nature.
- Limited power capacity at high range communications.
- Security and authentication.

In existing research, a secured, position aware and reliable mesh routing protocol was developed. In this research, PASER avoids the threats rather than IEEE 802.11 security mechanisms. In a real time environment of unnamed aerial vehicle (UAV) in wireless mesh network, the performance of PASER is better compared to IEEE 802.11 security mechanisms.PASER is Power Aware Secure Efficient Routing Protocol that aimed at improving the security of the routing method in unnamed aerial vehicle-wireless mesh network. This algorithm has improved the source verification to decrease the injury of the internal intruders that is to deal with the black-hole threats [8]. The energetic key supervision method of PASER has been used to adjust the key amount in all PASER data packets for better recognition of the key modifications. In previous research, route maintenance method has been updated in PASER.

C. Security objectives of PASER [9]

This algorithm aims to meet the three objectives which are listed as;

- Preventing external threats
- Dynamically removing malicious hops from the system.
- Reduce the damage of internal threats unless these have been removed from the system.

In contrast, PASER attempts at developing and preserving exact paths among legitimate hops. External malicious hops must be capable to control the routing method or connect the system. The hops must be removed from the system and keys must be updated dynamically. PASER recognises and avoids malicious conduct by which intruder diverges from the protocol sequence. To meet the security objectives, PASER follows some of the aspects like as data verification, data packet refreshment, nearest hop verification or authentication, source verification and dynamic key maintenance.

In this research work, discussed about the improved OLSR Routing protocol. In this research, routing is improved with the help of DES encryption method. In research work, the proposed method has enhanced the performance metrics and security factors with the help of Throughput rate, Delay and PDR (Packet Delivery Rate) in the WMN (Wireless Mesh Network).

Sections are described as follows- section I explained about the overview of the wireless mesh networks. Section II surveyed about different papers. Section III described about the attacks in wireless mesh networks. Section IV explained about the research methodology of the proposed work. Section V designed OLSR routing protocols in WMN. Section VI demonstrated about the experimental results. Section VII described the conclusion and future scope.

II. PRIOR WORK

aKim, J., Lee, S and Lee, S et al.,2018 [16] proposed research on a collection of the cluster ad hoc administration. The administration resolves the issue that took place in wireless mesh network. The installation of the wireless mesh network was not easy and no software mesh topology was required for the computerised software methods. In the final approach, there was no combined method for the management of the ad hoc network. This research focused on some of the issues of WMN and described it. In addition, this research analysed the performance of the communication flow controlling in wireless mesh network. The utilised software in this method was open source cluster ad hoc management scheme. **Yuhuai, P. E. N. G., Qingxu et al.,2019 [17]** implemented a novel code awareness routing technique with increased applications. The protocol helped in the creation of the possible coding, chances in the process of the development of the route. After that, a suitable route was selected with maximum coding between the access paths. Simulation was done using the NS2 simulator and parameters metrices were throughput, end to delay coding gain. It was noted that throughput value was 11%,and coding gain was 17% . **Panwar, L. C et al., 2017[18]** proposed research on different methods to resolve the problems of routing and safety for wireless mesh networks. The mesh network was distributed and self-configured kind of network where there was no central base station so need of the security, quality of service (QOS) and routing. Moreover, this research utilised different methods to solve the problems that was reviewed in existing research. **Naresh, S. and Singh,2016 [19]** Studied the wormhole threats in wireless mesh network and different threat detection methods. The different detection methods such as mutual data transferred, cluster based recognition, and recognition using node-count was also described. The other key solution was mutual data between connecting access points that avoids the rough points to work as neighbours. The positioned data and clock synchronisation, node count recognition recognised 75% threats in few minutes, two hop count nearest node recognition in wireless mesh network.

In table 1.described about the performance metrices utilised in WMN. The parameter values are analysed by comparing various surveyed techniques. Toorchi, N., et al., [17] computed the performance using time evaluation (delay) and network lifetime depends on throughput. Bao, K., et al., [23] evaluated the results through packet delivery ratio, delay and lifetime of network (throughput).

Table 1: Performance Metrics used in WMN (Wireless Mesh Network).

Author Name	Packet Delivery Rate(PDR)	Delay	Throughput
Kim, J., et al., [16]	X	X	X

Toorchi, N., et al., [17]	X	✓	✓
Panwar, L. C et al., [18]	X	X	X
Di Pascale, et al., [20]	X	X	X
Bao, K., et al., [23]	✓	✓	✓

Di Pascale, E., Macaluso, I., Nag, A., Kelly, M et al.,2018[20] investigated a research on the combination of the data and processing system. Fresh information was gathered by sensing the combined sensors and converts into suitable arrangements as it operates towards the system and activating hops. This research presented a component of the visualisation in which there was mapping the process of artificial neural network (ANN) for the communication of the multiple node and transmission of data. Through the principle of the locality features in internet of things applications, proposed method decrease the rate of latency during the communication. The calculation of the system was performed where the information transfers along the last receiver node, and this method was named as network as a computer. **Pawar, R., Munguwadi, V and Lapsiwala, P et al.,2018 [21]** demonstrated the problem of the common connection failures in wireless mesh network and their influence on the throughput, congestion rate and power dissipation. Generally, wireless mesh network was compared with the deep geographical area as compared to the predictable ad hoc system. In addition, wireless connections utilised the reliability standardisation for the media access and interconnection that was mainly exempt to distortion and interference. Hence, link and path management was a challenging issue for the scientists. This research studied the various features of the wireless mesh network, connection failure challenges, merits and demerits. Hence, wireless mesh network was used in the growth of the internet of things, electrical distortion scheme and other applications in industrial applications. **Li, K and Nabrzyski, J et al., 2018 [22]** addressed a research on inter- cloud interconnection in wireless mesh networks. They proposed two optimum approaches which recognise the maximum amount of the known virtual machine to form a cloud-network wireless system in similar and different cases. In addition, they designed other two optimum methods to decrease the entire inter cloud network announcement traffic in both same and different cloud-mesh network, correspondingly. In next approach, they studied the virtual machine assignment issue under the multiple scenarios where NP hard was demonstrated. Finally, a heuristic process was suggested to provide an effective result. In this research, they focused on the inter cloud mesh network communication where resultant value analysed the efficiency of the system. **Bao, K., Hu, F and Kumar, S et al., 2018[23]** presented research on routing methods for wireless mesh network appointed for the two features namely ripple diamond chain shape routing and artificial intelligence augmented route selection. A ripple diamond chain shape routing multiple transmission activity exploit data using rate less code to achieve loss resilient symbols for information packets that can be transferred at the same time in various beam of hops. Table 2 explained the various techniques, advantages and issues occurred in WMN. Various surveyed techniques has been evaluated along with issues and advantages. After that, they utilised ripples to distinguish every node in tree topology of wireless mesh network. The secret code was transmitted on multiple streams of light on the main route in one nipple. In other routing method, routing technique was improved through an artificial algorithm.Fuzzy logic was utilised to describe subjective link excellence to adapt to varying quality of service necessities. The strengthening learning method was utilised to select the main route based on the increasing repayment in all the connections. Simulation was done using video along with time sensitive traffic to compute the efficiency of routing and selection of the route in wireless mesh network.

Table 2: Elaborates the several methods , benefits and Issues Occurred in WMN (Wireless Mesh Network).

Author	Year	Technique	Advantages	Issues
Kim, J., et al., [16]	**2018**	Gathering of Organization Treating Humble-hoc Management (GOTHAM)	Cost effective software system. Mapping information.	Complex system
Yuhuai, P. E. N. G., Qingxu et al., [17]	**2019**	Coding based routing protocol method	Reduced delay and energy consumption, maximum throughput.	Channel fading, distortion, limited resource frequency.
Panwar, L. C et al., [18]	**2017**	Flooding propagation method	Detection of DDos attack.	Security and quality of service issue.
Di Pascale, et al., [20]	**2018**	Artificial Neural network (ANN)	Better communication and reduce latency rate.	Complexity.
Pawar, R., Munguwadi, et al., [21]	**2018**	Wireless broadband technology	Connection failure.	Industrial applications.
Li, K et al., [22]	**2018**	Inter cloud –net communication Method	-	Multiple channel communication issue.
Bao, K., et al., [23]	**2018**	Ripple diamond chain shape routing and artificial intelligence augmented route selection	Better communication	Complexity
Naveen, T. H. et al., [24]	**2017**	Multi-bound and pro-active technology.	System control and management for reducing complexity.	Quality of service (QoS) concern, network distribution, sustainability of directions

Naveen, T. H. and Vasanth, G et al.,2017 [24] reviewed some of the existing methods to avoid the issues that were related to transmission and searched for the open issues.
This research described the routing methods for wireless mesh system. In addition, the main feature of wireless mesh network routing achieved better output for the adjustable load. Along with that, also surveyed various methods of the wireless mesh network and compared with the existing methods.

III. ATTACKS IN WIRELESS MESH NETWORKS

Wireless mesh network is used to offer the internet connection as a common approach for wireless internet service suppliers due to simplicity and less- cost system distribution[11]. In this section, described the detailed study of attacks in wireless mesh networks(WMN) [12].

(i) Black-hole attack: It is one of the major security attacks in wireless mesh network. Generally, attackers use the ambiguity to process the malicious conduct for the reason that route investigation is essential and unavoidable. Various scientists have accompanied various detection methods to develop various kinds of the detection methods [13].

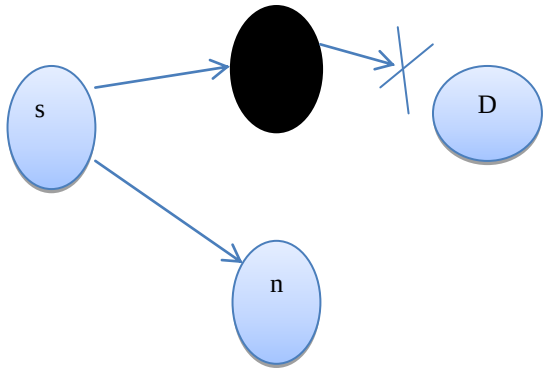

Fig 2. Black Hole Attack

(ii) Wormhole Attack: Generally, intruder catches data packet at one position and passageways to another position. The generated passageway is known as wormhole threat. This may be the serious kind of attack to routing protocols that may affect route investigation method of delaying the investigation of any path other than worm-hole [14]. As given in fig 3, an unnecessary connection is made from B to C by attacker hop Y.

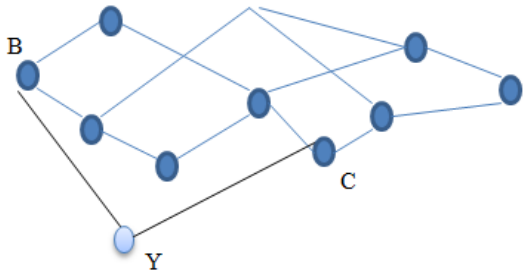

Fig 3. Wormhole Attack

(iii). Gray-hole Attack: This attack is a dynamic, information traffic , route layer threat. Gray-hole hop is one which acts as black hole hop from time to time that works as intruder and drop the data packet. Hence, it can be realised as differentiability on black hole threat [15]. In WMN , susceptibilities of S/W in movable operating system enable mesh routers more susceptible to such threats. Hence, an intruder may drop data packets by physiological capturing of the hops as hops may be fixed on top of the roofs.

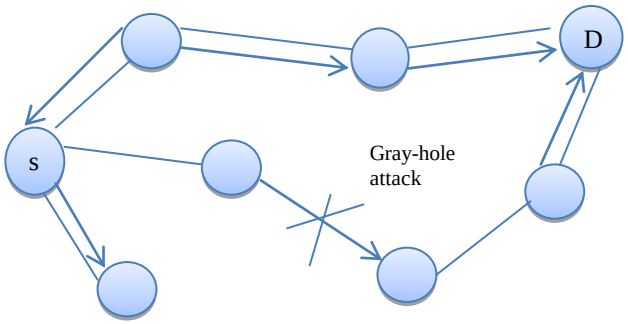

Fig. 4 Grey-Hole Attack

In table 3 demonstrated various types of attacks and security techniques on various layers of the wireless mesh network(WMN) .

Table 3: Different attacks and security methods based on different layers of the network

Layers	Attacks	Security methods
Physical	Jamming attack	Priority data packets and mapping of areas.
MAC	Collision of nodes, unfairness	Error correction codes, small frames.
Routing	Black hole, gray hole attack, Worm hole attack	Monitoring of the geographical data.
Network layer	Spoofing, black hole and sink hole	Redundancy checking and verify authentication.
Transport	Logical Faults,	Trusted authentication

IV. RESEARCH METHODOLOGY

In this research methodology work, upgraded novel method to include a route maintenance mechanism that calculates the following phases.First, it dealt with the deployment of the network, which deals with the calculation of network area and spreading of nodes in the network. Then, it will see the registration process with the key distribution center for UAV's and it is related to the transmission of packets in the encrypted form and see the authentication of the routes. It implemented the secret key algorithm for authentication phase because of secure data transfer one node to other nodes. It performed the attack on the network through performance of the network in the presence of the attack can be analysed. If Attacker node detects, then implement the routing and optimization approach for secure data transmission and less packet loss and delay. An optimization of the network is required and then we optimize the network and then evaluate the performance of the network in terms of throughput, end delay, packet delivery rate, energy consumption of the network.

Steps in WMN using Routing Protocol:
Enter the Mesh Node in the Wireless Mesh Network.
Calculate the Area (length * Width).
Calculate the Energy of the Mesh Node in the network.
Data Center in the network.
Authentication
Packet Transmission
Encryption Phase
Decryption Phase
Find Attack (Wormhole and DDoS)
Trusted Mesh Node
Implement an OSOLSR Algorithm
Performance Metrics.

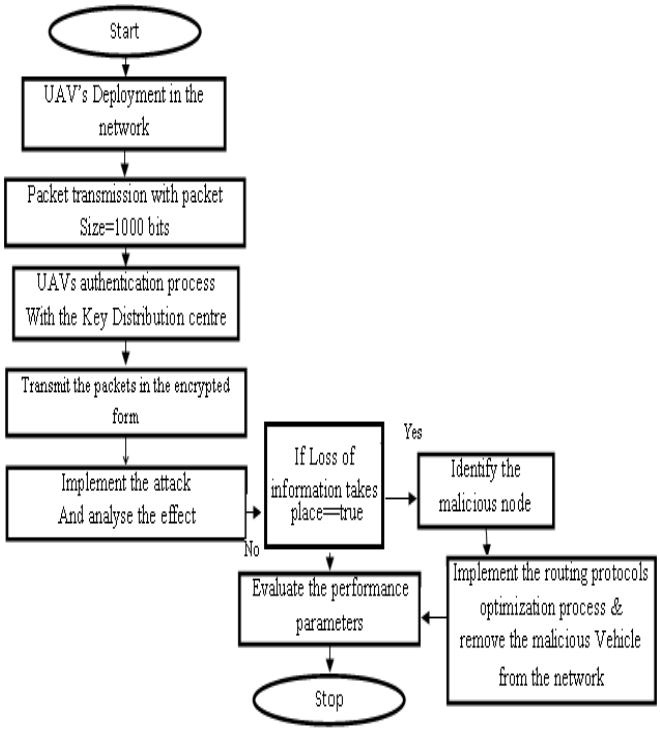

Fig 5. Research Methodology Flow Chart

V. DESIGNED OLSR ROUTING PROTOCOL IN WMNs

In this section , elaborate the research method which is implemented in wireless mesh networks. In existing work ,designed PASER algorithm to consider the network position and improve the delivery rate 70%. But 30% loss occurs cause oof black hole attack. In research proposal, discussed a novel protocol to improve the end to end delay, delivery rate and recover the loss of the information from the source to a destination node in the network. In under section described about the routing protocol in detail described.

A. OLSR Routing Protocol

OLSR routing Protocol is an optimized link-state routing protocol developed for Wireless Mesh Networks (WMNs). An optimization depends on a method is called optimized multi-point relaying. The mesh nodes are selected as a multi-point relaying and re-transmitting manage messages. Multi-point relaying method is used to reduce the network overhead and also optimized the content of control packets because the data that is flooded in the mesh network is restricted to data of multi-point relaying's.

In other words, the mesh nodes that are not chosen as a multi-point does not flood and re-transmit any broadcast messages.
An individual mesh node in the network transfers and signal broadcasts control messages intermittently. Since the frequency of these control messages is high, the occasional packet loss of some packet controls can be tolerated. Therefore, no re-transmission is required for loss of packets. Two kinds of basic control messages OLSR routing protocols are :-

- H-Messages
- T- Messages

H-Messages are occasionally interchanges among one-hop neighbors. The individual mesh node broadcasts its Identity (ID) and its single –hop neighbor table to its nearest nodes with Time-To-Live equal with one. These messages allow an individual node to get information about its nearest option binary hops. Upon receiving an H-message , the mesh node records the information of the H-message in its nearest table. The nearest table of a mesh node named A comprises following area :

- Mesh_node_address :- Identity (ID) of H-message sender. It is a single-hop neighbor of node A.
- Status of Mesh Node:- The connection status code.
- Hop-list in mesh node:- The record of single-hop nearest of address (ID) sender of messages that are measured as 2-hop neighbors of node A.
- Time of Mesh Node: - The interval time that this access will be reserved at neighbor table.

MRP in the mesh network occasionally signals broadcasted a message is called as a T-message. T-message are transferred through MRP mesh nodes to all nodes in the network for flooding network's topology data.

V. EXPERIMENTAL RESULTS

In this section, described about the result analysis with OLSR and PASER routing protocol. It provided the 'source' authentication in order to proactively minimize the harm of internal attackers i.e. to combat the "Fabrication" and "Blackhole" attacks. The author has generated a network of l000 *1000 meters. UAVs in WMN is taken in between 0 to 30. In the network, the author has calculated the area, normal energy of each node, normal ID and KDC (Key Distribution Center). The network operator runs a secure KDC that is responsible for dynamically manageable network credentials. At any given instant, mesh gateways can establish a reliable connection with the KDC and vice versa. In UAV-WMN, this can be realized by running the KDC. It is assumed that the legitimate nodes incorporate a positioning device that runs a secure navigation service as shown in Fig-6.

Table 4: Simulation Parameters

Requirements	Values
Network Deployment Area	1000*1000
Number of UAV	0-30
Packet Size	1000 bits

Source UAV	15
Destination UAV	5
Trusted UAV	15,2,3,14,5
Attacker Nodes	12
Parameter Metrics	Routing Delay, PDR and Throughput and Probability Distribution Function
Power Levels	50,60,70,85

Table 4 described that the detailed summary in simulation parameters (Requirements and Values). Network area defines 1000*1000 meters. A number of the UAV is like as an input vehicles. Packet size 1000 bits,find start node 15 and sink node 5. Implement a Base paper technique which is encryption process and registration phase done by KDC (Main Header) calculated the trusted UAV nodes 15,5,2,3,14. If packet transferring one UAV to Another UAVs. Then Packet transferring takes a lot of time and energy then packet loss at some point. Such an issue in the WMNs and attacked node found which is 12. We calculate the performance metrics like as a Routing Delay, Packet Delivery Rate, Throughput and Probability Density Function.It has upgraded PASER to include a route maintenance mechanism that calculates the following:-

Number of routes: Search route.(SCR---SOURCE NODE, DST—DESTINATION NODE).
Packets transfer: (i) Packets are transferering from UAV-IDs-15, 2, 3, 12, 14, 5 and (ii) Node 15 is Source node, Node 5 is Destination node (Refer to Fig-6).
Registration Process: After finishing the registration process, a node possesses the required symmetric network keys to successfully operate in the network i.e. Encryption technique (private and public key).
(i) Encode by DES algorithm
(ii) Decode by DES algorithm
There is a Secret key generation on the basis of DES algorithms. Trusted routes (15, 2, 3, 14, 5) (Refer to Fig-1) are developed in the network and thus Secure communication is possible with KDC assigned IDS in character format. Signal representation based on trusted routes and secures the communication.
Calculate the maximum energy of the network and each node in the network, if both the energies are equal, then there will be chance of the attacker to manipulate the routes in order to sabotage the network or to mount advanced attacks violating the flight security of the UAVs. Hence, author applies the attack on behalf of the energy. This attack is mostly wormhole attack in UAV-WMN. Node 12 is an attacker node as shown in Fig-6.

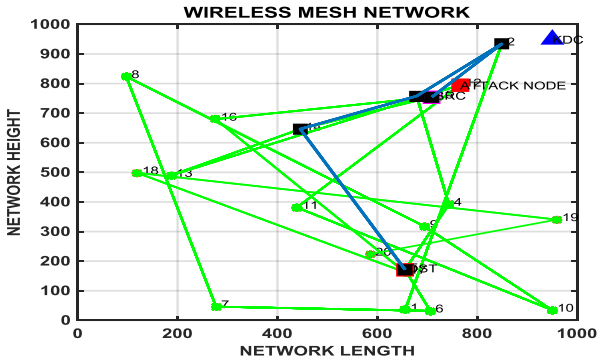

Fig 6. Deployment of the Network

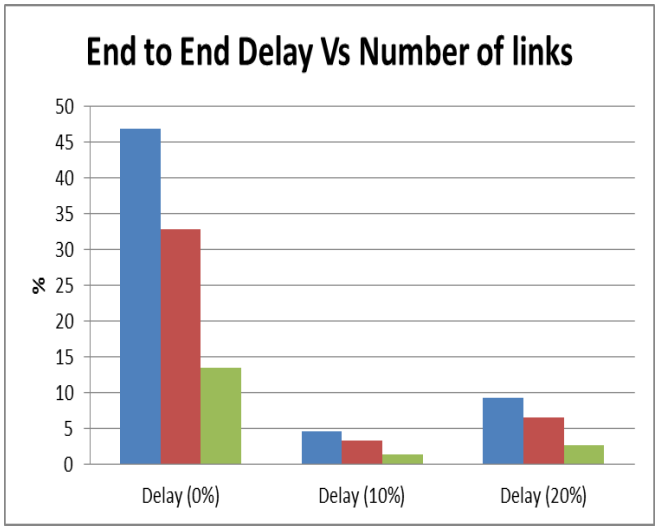

Fig 7. End to end delay vs num_of_links

Delay is calculated based on the frame error rate at 0%, 10%, and 20%. The results show only a slight increase of the route discovery delay of PASER while the number of links is multiplied, and the FER is increased. It is shown that Non-Considerable Delay Increases while increasing the FER as shown in Fig-7. Thus the network is Efficient and Robust.

Table 5 : Routing Delay in existing Work (PASER Routing Method)

Number of Links	Delay (0%)	Delay (10%)	Delay (20%)
1	46.9	4.69	9.39
3	32.9	3.29	6.58
5	13.52	1.352	2.704

Table 5 and 6 above described that the performance metrics which is Routing Delay (ms), vs Frame Error Rates, Throughput (%) and PDR (Packet Delivery Rate) Percent vs Time (s).

Table 6: Performance Metrics in PASER Approach

Performance	Values
Routing Delay 0%,10% and 20% (ms)	47.9,4.79,9.58
Throughput (Per cent)	0.81 ~ 81 %
Packet Delivery Rate (Per cent)	0.70 ~70 %

In Routing Delay calculated based on the Frame error rates based and level divided 0%, 10% and 20%. In packet Delivery and Throughput achieves the values are 70% and 81%.

VI CONCLUSION AND FUTURE SCOPE

Wireless mesh network is an organised network to deploy the large communication system and connects separated heterogenous system. It is not easy to deploy and manage the nodes of the wireless mesh network as it is based on the network scenarios. Moreover, it is necessary to organise wireless mesh network because it is required in emergency conditions and disaster managements. Deployment and management of the WMN tools are ineffective and consume maximum time. This research work proposed an enhanced OLSR routing protocol to enhance the performance of the UAV in wireless mesh networks. In WMN are concluded and used OLSR is an advanced version of the pure link state routing protocol and it is based on the multiple point delay(MPR) nodes. These are the selected hops that preserves the two nearest hops and decrease the rate of flooding of broadcasted data packets by decreasing the amount of the hops that re-transmits the data packets. In OLSR, the path is established from MPR nodes that work as mobile clients . Hence, the route that contains movable clients are not static hops. However, improved –OLSR is proposed to improve the performance of the UAV in wireless mesh networks. Routing protocol has improved the network performance based on packet delivery rate and DES encryption method used to secure the packet transferred from source to destination UAV. Data encryption standard is the major area of research for improving the security of the network and it is called as symmetric crypto-system. It is similar to encryption and decryption. DES may be threatened by various kinds of the cryptanalysis due to equivalent processing. It has concluded the secret key algorithm for authentication phase because of secure data transfer one node to other nodes. It performed the attack on the network through performance of the network in the presence of the attack can be analysed. If Attacker node detects, then implement the routing and optimization approach for secure data transmission and less packet loss and delay. An optimization of the network is required and then we optimize the network and then evaluate the performance of the network in terms of throughput, end delay, packet delivery rate, energy consumption of the network.In future work, will implement the EOLSR Routing with Highly optimization encryption method. It will process the registration phase to generate the trustworthy UAVs and assigned the Unique_ids. The packet will transfer source to destination UAV. It will data transfer high security and confidentiality in the military areas in the WMN (Wireless Mesh Networks).

REFERENCES

1. Li, J., Silva, B. N., Diyan, M., Cao, Z. and Han, K. (2018), " A clustering based routing algorithm in IoT aware Wireless Mesh Networks", Sustainable cities and society, vol.40,pp. 657-666.
2. Yu, G., Zhang, J., Leung, V. C., Kountouris, M. and Wang, C. (2018), IEEE Access Special Section Editorial, " Mobile Edge Computing for Wireless Networks", IEEE Access, 6, 11439-11442.
3. Sowmya, C., Naidu, C. D., Somineni, R. P and Reddy, D. R. (2017), " Implementation of wireless sensor network for real time overhead tank water quality monitoring" ,In 2017 IEEE 7th International Advance Computing Conference (IACC) (pp. 546-551). IEEE.
4. Mahmood, K., Nazir, B., Khan, I. A and Shah, N. (2017), "Search-based routing in wireless mesh network" ,EURASIP Journal on Wireless Communications and Networking, 2017(1), 36.
5. Liu, F and Bai, Y. (2012), " An overview of topology control mechanisms in multi-radio multi-channel wireless mesh networks" ,EURASIP Journal on Wireless Communications and Networking, vol. 2012(1),pp. 324.
6. Singh, M. (2019), " Wireless mesh networks architecture. In Node-to-node approaching in wireless mesh connectivity (pp. 11-14). Springer, Singapore.
7. Tsao, S. L., Su, J. J., Huang, K. L., Shih, Y. C and Tseng, C. C. (2014), " An end-to-end channel allocation scheme for a wireless mesh network" ,International Journal of Communication Systems, vol. 27(12), pp. 4407-4429.
8. Sbeiti, M., Goddemeier, N., Behnke, D and Wietfeld, C. (2015), "PASER: secure and efficient routing approach for airborne mesh networks", IEEE Transactions on Wireless Communications, 15(3), 1950-1964.
9. Sbeiti, M., Pojda, J and Wietfeld, C. (2012), " Performance evaluation of PASER—An efficient secure route discovery approach for wireless mesh networks", In 2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications-(PIMRC) (pp. 745-751). IEEE.
10. Akyildiz, I. F and Wang, X. (2005), " A survey on wireless mesh networks", IEEE Communications magazine, vol. 43(9),pp. S23-S30.
11. Varatharajan, R., Preethi, A. P., Manogaran, G., Kumar, P. M. and Sundarasekar, R. (2018), " Stealthy attack detection in multi-channel multi-radio wireless networks", Multimedia tools and applications, vol. 77(14),pp. 18503-18526.
12. Hossain, M. and Xie, J. (2018), " Off-sensing and route manipulation attack: A cross-layer attack in cognitive radio based wireless mesh networks", In IEEE INFOCOM 2018-IEEE Conference on Computer Communications (pp. 1376-1384). IEEE.
13. Tseng, F. H., Chou, L. D and Chao, H. C. (2011), "A survey of black hole attacks in wireless mobile ad hoc networks", Human-centric Computing and Information Sciences, 1(1), 4.
14. Jan, S. U., Ahmed, S., Shakhov, V and Koo, I. (2019). Toward a Lightweight Intrusion Detection System for the Internet of Things. IEEE Access, 7, 42450-42471.
15. Khan, S., Loo, K. K., Mast, N and Naeem, T. (2010), " SRPM: secure routing protocol for IEEE 802.11 infrastructure based wireless mesh networks", Journal of Network and Systems Management, 18(2), 190-209.
16. Kim, J., Lee, S and Lee, S. (2018), " Mesh Network Convergence Management System Using Software-Defined Network", Mobile Information Systems, 2018.
17. Yuhuai, P. E. N. G., Qingxu et al., (2019), " A New Network Coding Based Routing Protocol for Enhancing Throughput Capacity in Wireless Mesh Networks", Chinese Journal of Electronics, vol.28(2), pp.416-422..
18. Panwar, L. C. (2017), " Techniques of wireless mesh networks-a review", International Journal of Advanced Research in Computer Science,vol. 8(7).
19. Naresh, S and Singh, E. N, "A survey on wormhole attacks on Wireless Mesh Networks and its detection".
20. Di Pascale, E., Macaluso, I., Nag, A., Kelly, M and Doyle, L. (2018), " The network as a computer: A framework for distributed computing over IoT mesh networks", IEEE Internet of Things Journal, vol. 5(3), pp. 2107-2119.
21. Pawar, R., Munguwadi, V and Lapsiwala, P. (2018), "Wireless Mesh Network Link Failure Issues and Challenges: A Survey", International Journal of Scientific Research in Network Security and Communication, vol. 6(3), pp. 28-36.
22. Li, K. and Nabrzyski, J. (2018), "Virtual machine placement in cloudlet mesh", Journal of Communications and Networks, vol. 20(3), pp. 266-278.
23. Bao, K., Hu, F and Kumar, S. (2018), "AI-Augmented, Ripple-Diamond-Chain Shaped, Rateless Routing in Wireless Mesh Networks With Multibeam Directional Antennas" ,IEEE Access, 6, 24311-24324.
24. Naveen, T. H and Vasanth, G. (2017)., "Qualitative study of existing research techniques on wireless mesh network", International journal of advanced computer science and applications, vol. 8(3), pp. 49-57.

AUTHORS PROFILE

Jasleen Kaur received the B.Tech degree in Electronics and Communication Engineering from SUSCET Tangori, Mohali, India, in 2011, and the M. Tech. degree in Electronics and Communication Engineering from Chandigarh Engineering College, Landran, Punjab, India in 2013 and the is presently perusing Ph.D degree in Electronics and Communication Engineering from Shri Jagdish Prasad Jhabarmal Tibrewala University, Rajasthan, India. She is the author of 04 journal and conference papers. Her fields of interest include Image signal processing and wireless communication.

Dr. Om Prakash received the AMIETE degree in electronics and telecommunication engineering from IETE, New Delhi, India, in 2008, and the M. Tech. Degree in Instrumentation and Control engineering from Sant Longowal Institute Of Engineering And Technology, Longowal, Punjab, India in 2010 and the PhD degree in electronics and communication engineering from Shri Jagdish Prasad Jhabarmal Tibrewala University, Rajasthan,India in 2015. At present working with St. Mary's Engineering College, Hyderabad, India in the capacity of Associate Professor in Electronics and Communication Department. He is the author of more than 50 journal and conference papers. His fields of interest include power system optimization, Image signal processing, Antenna design, Embedded system and wireless communication. He is the Member of Scientific and Industrial Research Organization, IETE, Delhi and International Association of Engineers (IAENG), Hong Kong.