IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-6, Issue-3 E-ISSN: 2347-2693

An Improved Security Network Life Based on Data Ant Colony Optimization Method Used in Wireless Mesh Network

Paramjit Kaur [1], RakeshKumar[2]and Harinder Kaur[3]

[1*]Department of CSE,SECG, Gharuan, India
[2]SECG, Gharuan, India
[3]Department of CSE, SECG, Gharuan, India

Corresponding Author:rakesh77kumar@yahoo.com

Available online at: www.ijcseonline.org

Received: 12/Feb//2018, Revised: 20/Feb2018, Accepted: 15/Mar/2018, Published: 30/Mar/2018

ABSTRACT- In wireless technology, the devices communicate with each other without physical connections. It gives together merits and demerits when evaluated to a wireless technology. In this research work, we have studied the DSDV, AODV, DSR and ZRP routing protocol comparison. The encryption technique has implemented the security in the mesh networks. We have implemented the secret key encryption algorithm. This algorithm uses a dissimilar key for encoding and decoding. The decoding key cannot derive from the encoding key. Main focus on this research work as to identify the wormhole attacker node in the network with the help of Secret Encryption Algorithm and prevention using Data Ant Colony Optimization algorithm. We have used the MATLAB 2013a simulation tool with SCRIPT Language. We calculated the performance parameters, i.e. throughput, packet delivery rate, probability distribution vs. time and delay vs. Frame error rate [ms].

KEYWORDS- Wireless Mesh Network, Data Ant Colony optimization, Secret Encryption Algorithm, Wormhole attack and routing protocol.

I. INTRODUCTION

The Wireless Mesh Network is a novel wireless networking model. Basically, wireless internet service sources are selecting wireless mesh network to give internet connectivity, as it provides an easy, fast and costly network development [1].A Major challenge to implement these networks is their vulnerability to security attacks. Wireless Mesh Networks are suitable for fields that don't have previous data capabilities for the deployment of the normal wireless network [2].Wireless Mesh Network has been an area of active research in current years. However, the research has been intensive around several protocols for multi-hop routing, leaving the field of security un-explored. At the same time, new limitations of WMN are radio access networks in rural or metropolitan fields, wireless community and wireless backbones for procedure automation, etc. The introduction requires more security mechanisms and strong privacy protection. The connectivity between mesh nodes in WMNs is automatically maintained and established among the participating nodes. It makes wireless mesh network a dynamic, self-configured and self-organized wireless network [3].Wireless mesh network advantages are low cost installation, large scale development, reliability and robustness etc. In WMN deigns, the routing protocol confirms security algorithms of the individual links of multi-hop connection. End to end security has to be developed at the application layer. However, it is needed to secure the less critical application information and mesh protocol tracking from out-side hijackers.WMN topology has a divided style. As the architecture becomes more complex, the security problems in the network increase [4].Wormhole Attack is relatively serving, and consists in footage traffic from one district of the network and repeating it in different areas [4].It detects the various worm hole nodes, creates a fake route that is smaller than the original data route within the network. This could complicate routing structure which relies on the information regarding distance between nodes. The wormhole attack node has one or more duplicate nodes and tunnel between them. The attacking node captures the information about the distance between nodes and transmits to another located node which divides them locally.

Resolving methods for security problems in WMN are:

- Router client Authentication
- Router client key agreement
- Client to client authentication
- Client to client key agreement and
- Position privacy.

II. RELATED WORK

Aggeliki et al. (2013)[5] In this paper, a survey on mesh networks in wireless communication. The mesh network technology can save much more cost for communication as compare to other networks. It is a high speed network, which can be a combination of various other topologies.

Perrig et al. (2014) [6] Surveyon various security issues in the wireless networks along with their some routing challenges. Author investigated their research with some attacks in the wireless networks. Attacks can degrade the performance of the network. They stole information with many anonymous routes in the network. Different attacks are having their own way to perform degrading on the network. Some of them are working with some kind of clone node and pushing a heavy load on the network. These types of attacks are known as DDOS attacks. DDOS attacks applied through a heavy load of request pushing on the server, which damaged by the processing speed of the network.

Kato et al. (2015) [7] Described the process, there are many unmanned aircraft systems and ground base stations are configured. These are responsible to create a UAS network and communication of data packets from one to another node. In this paper author investigate some problem during setup and operating this type of terminology. This problem causes high operating cost and maximizes the time consumption of network communication.

Borhanuddin et al. (2015) [8] Researched on WMN with the mesh topology organization of various nodes and radio transmission. Authors choose this network due to their behaviour. It has ability to join the various networks in a particular system to transmit data efficiently. In this research the author also integrated mesh network with Wi-Fi technology on the basis of some IEEE standards like IEEE801.11 etc. Another approved IEEE standards used to verify the quality of services in the mesh networks. In this research author enhanced previous work and make it compatible with TDMA/TDD with quality of service enhancements as well.

Wang et al. (2015) [9] In this research ULNC scheme is purposed in the field of wireless mesh networks. Author worked on the basis of two major problems in the WMN as tracking the flow of data and their movement. These are the major part of transmission, which can help to prevent attacks on the network. To reduce the attacks on the network the encryption technique can help for secure transmission of data from source to destination.

Sbeiti et al. (2016) [10] Researched on the mesh network with some security issue. Author proposed an approach called position aware secure and efficient mesh routing approach. In this paper the network node are air vehicles which are used with a secure communication and provide efficient transmission. UAV's are unmanned air vehicles which can be used in some critical situation to provide the environmental gesture of information to the control room.

Akilarasu et al. (2016) [11] Security in mesh network is always a challenging work. Attacks like -hole can create some anonymous routes or node virtually in the network to distract the transmission of the network. As same the other attack can also degrade the performance with applying the heavy load on the network. Some anonymous nodes send lots of requests on the network and the network suffer with heavy request load. The heavy load can delay the actual transmission in the network and some reasons.

Table 1.Summarized by the techniques and Performance Parameters

Author Name	Year	Technique Used	Parameters
Aggelikiet et al.	2013	Encryption	Throughput
Perrig et al.	2014	AODV and DSR	Throughput
Kato et al.	2015	Optimization	Energy and Throughput
Moh et al.	2015	TDMA and TDD	Loss Probability, Throughput, Etc.
Wang et al.	2015	Linear Network Coding	Loss Probability, Throughput, Etc.
Sbeiti et al.	2016	PASER routing protocol	Delay packet delivery
Shalinie et al.	2016	Routing protocol	Throughput and Packet Delivery

III. Routing Protocols

Wireless Mesh Networks traffic is accepted to large volume and mainly between IGWs and Multi-Relay which positions larger demand on the main paths associated gateways and routers. The structure of wireless mesh networks required main focus on aspects such as adding multi-way routing, load balancer, traffic control and divide policies and scalability and among others. Since of some common characteristics among WMNs and Mobile's Networks, routing protocols implemented for Mobile networks are also applicable for wireless mesh networks. Some use of routing protocol in WMNs is a DSDV routing protocol, DSR, AODV and ZRP etc. [12].

Table 2.Characteristics differences in Routing Protocols

Characteristics	Dissimilarity
Network Topology	Fixed wireless back-bone
Traffic Design	Traffic can flow b/w any pairs of nodes

Inter path interference	Issues of hidden and exposed terminals
Link Capacity	Sensitive
Channel Diversity	WMNs could merits from the possibility of defining channel diversity in routing process.

Table 3. Difference between routing protocols

Routing Protocol Name	Type	Working
Destination Sequence Distance Vector	Table Driven	Requires a regular update of its routing tables. DSDV isn't suitable for largely dynamic networks.
Dynamic Source Routing	On demand protocol	Route discovery and maintenance
Ad hoc on-demand distance vector	On-Demand protocol	Build routes using route request and reply query phase.
Zonal Routing Protocol	Table driven	Uses proactive within a k-hop routing zone and employ a re-active routing approach beyond the routing zone.

IV. PROBLEM FORMULATIONS

Various papers studied and found and issues in research distance in a Wireless Mesh Network like network development and safety issues. In network development, there are several abilities of routers or gateways and there are no issues between routers [13]. Routers are not rotated and have multiple radio transceivers, which allow them to inter connect suddenly with more than one neighbour at the same time using dissimilar channels. Transmission power or distance range of routers can be caused by an understated set of possible ranges. The node request of hosts is collected per node. These hosts are in the transmission range of the node distance. The future model can be used division for users' coverage. Each router is replaced by a host with a request [14]. The hacker can operate the information and attract all the contents and misuse the UAV's due to which there are lots of risks of reducing packets [15] by the hacker or outsider. The hacker can loss the route and produce the fake /duplicate route and makes the vision of each packet to portable on that fake/duplicate route [16]. A hacker can harvest the multiple fake traffic copies (IDs) of the Unmanned Aerial Vehicle to enhance such as the packet, throughput of the network advance and reduce the network lifetime which affects the route detection delay in the network [17].

V. PROPOSED MODEL

In this chapter, we discussed the proposed model with key points and phases.

V.1 Proposed Key-points

1. To Study of a variety of encryption based safety algorithms.
2. To implement the registration process in Unnamed aerial vehicles using the Key distribution centre. To secure the network using encryption techniques used for detecting the attacker node (Worm attack).
3. To propose Ant Colony Optimization Approach for secure packet delivery and prevent the malicious node.
4. To evaluate the proposed parameters like Packet Delivery Rate, Throughput and End to End Delay and compare its existing performance parameters.

V.2 Explanation of wireless networks using data ant colony optimization

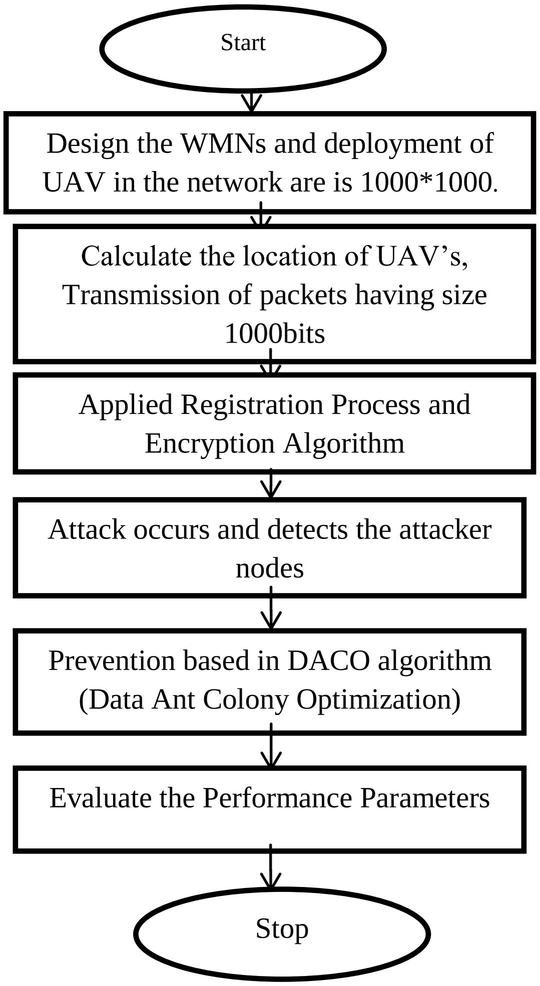
Start
Design the WMNs and deployment of UAV in the network are is 1000*1000.
Calculate the location of UAV's, Transmission of packets having size 1000bits
Applied Registration Process and Encryption Algorithm
Attack occurs and detects the attacker nodes
Prevention based in DACO algorithm (Data Ant Colony Optimization)
Evaluate the Performance Parameters
Stop

Figure 1 Proposed Flow chart

Phase I. First, we create the wireless mesh network, which connects one UAV node to another UAV node. To communicate the information in connecting form, this is linked together.

Phase II. Next, we search the source and destination node in this network. We plot the Main Head node name is Key Distributed Centre.

Phase III. In 'Main Head' normal id's and unique id's as created in the wireless mesh networks to travel on position to another position in the mesh networks.

Phase IV. The purpose of unique id is Main Head communicates a secure message and send the trusted node, which is defined by the KDC administration.

Phase V. KDC administrator provides authentication by means of the registration process. Limit decided is the 20 - 50 Unnamed Aerial Vehicles. If any other user who crosses the limit, then message will be displayed by KDC (not authorized Unnamed Aerial Vehicles).

Phase VI. We implement the encryption technique to provide the security in the mesh networks. We implement the secret key encryption algorithm. The secret key algorithm is implementing a security which provides the similar key to encode and decode data. This algorithm uses a dissimilar key for encoding and decoding, and the decoding key can't derive from the encoding key.

New Secret Key Algorithm could be separated into binary types:

a) Stream-ciphers
b) Block-ciphers

In stream cipher, a single bit of plaintext is encoded at a time**,** whereas block-ciphers offer a number of bits, i.e., normally 64-bits in new ciphers and encode them as an individual unit.

An encryption technique is used for detecting the worm hole attack in the WMNs.

Phase VII. We calculate the performance parameters based on the PASER (Power Aware Secure, Efficient Routing Protocol) with Encryption Techniques (Distance Probability, Throughput, packet delivery rate and frame error rate based on delay (0%, 10% and 20%).

Phase VIII. We implement the proposed approach named as an Ant colony optimization algorithm. This is resolving the network issues and transmits the data securely and calculates the performance parameters, i.e. throughput, delay and delivery rate etc.

Phase IX. Comparison between the existing and proposed approach and proved that proposed work is better than previous one.

VI. RESULTS AND DISCUSSIONS

In this section, we design the wireless mesh networks. We discussed the result explanation in wireless mesh networks.

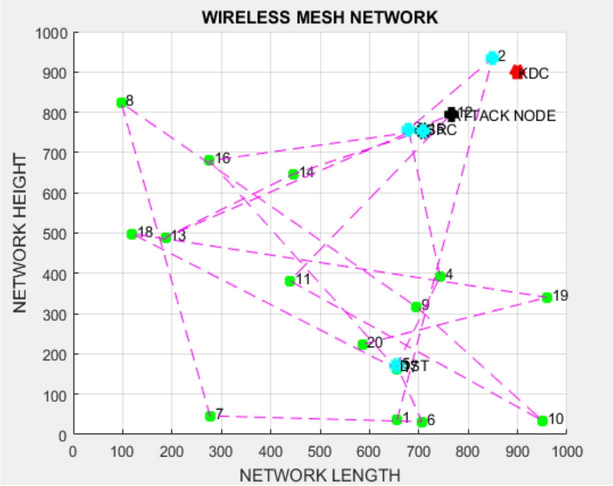

Figure 2 Wireless Mesh Networks

In this figure 2, the MESH system connects the UAVs (Unnamed Aerial Vehicles)for the broadcast of packets from source (S) to the destination (D) in which source or destination is planned in red or green color or all other nodes with thirst. The trusted node represents the wireless mesh network. Trusted Node registered through the Key distribution centers. Message box defines that the Unnamed Air Vehicle are authorized vehicles and registration is completed by the KDC. The packet will be delivered or transferred from unnamed air vehicles.

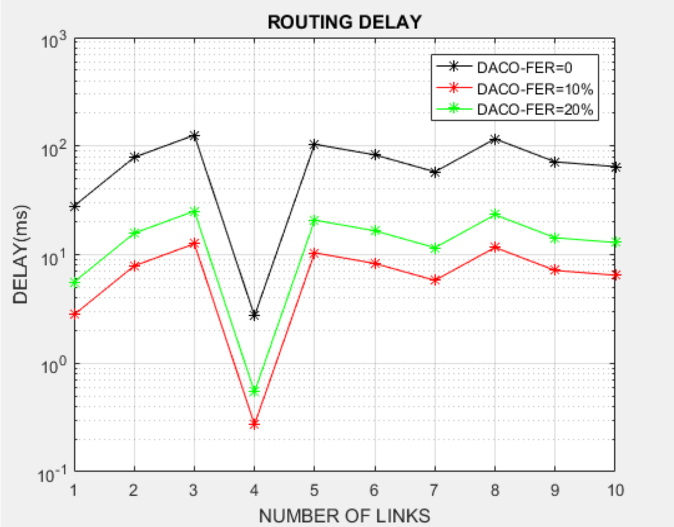

Figure 3 End to End Delay (Proposed Work)

The figure 3 shows the routing delay to transmit the data like packets from source to the destination having FER which is the frame error rate (FER) in DACO. These are viewing the delay in between the transfer of the data packets when the FER is 0%, FER is 10 % or FER is 20%. Less delay results in the high Packet Delivery rates.

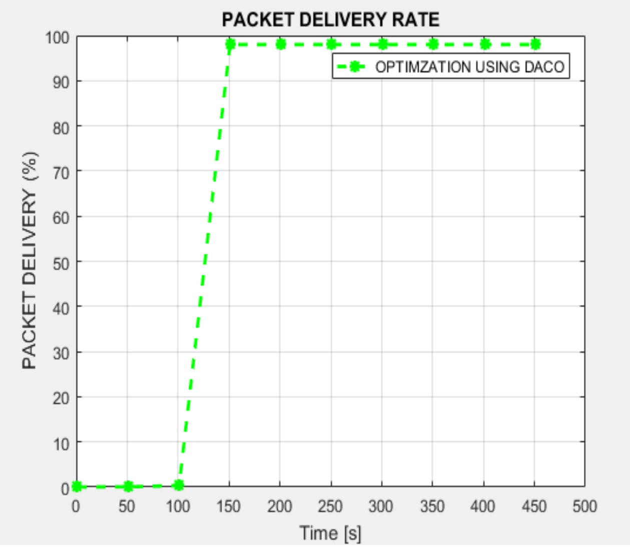

Figure 4 Packet Delivery Rate (Proposed Work)

The figure 4 illustrations above the packet delivery rate (PDR) for the successful transmission of data packet from source to the destination through secure trusted vehicles which appearances that 98%delivery packets are communicated using secure transmission.

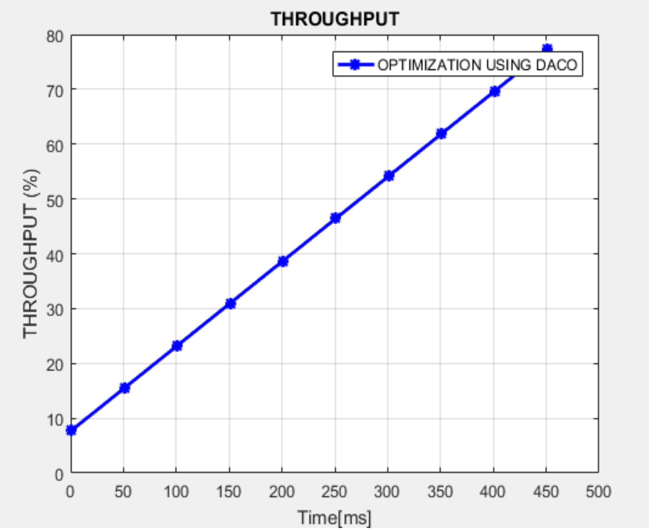

Figure 5 Throughputs (Proposed Work)

The figure 5 illustrations above throughput for the positive transmission of data packets from source to the destination through secure trusted vehicles which shows that 79% throughput with DACO are communicated using protected transmission.

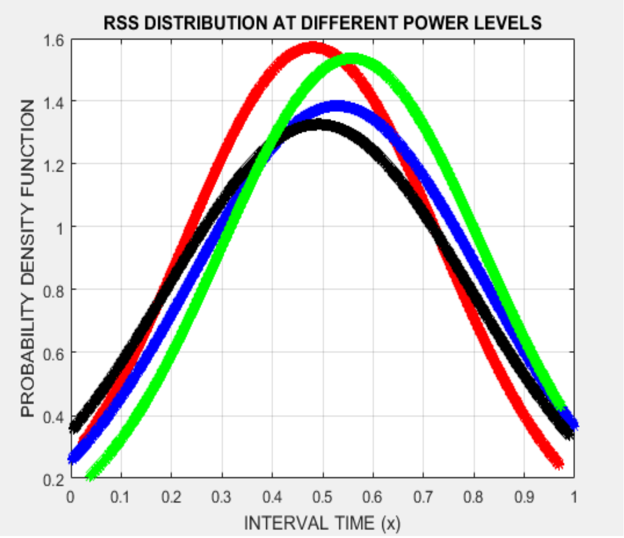

Figure 6 RSS Distribution at Different Power Levels

The figure 6 shows the probability density function (PDR) in DACO which shows the probability of getting the path destruction when attacker attacks in the systems or the red line shows the regular probability for the designed system function.

Table 3. Proposed Performance Parameters

Performance Parameters	**Values**
Delay 0%	64.63ms
Delay 10%	6.4ms
Delay 20%	12.93ms
Throughput	79%
Packet Delivery rate	98%

Table 4. Comparison between Throughput (Proposed and Existing Work)

Time [ms]	**Throughput-DACO**	**Throughput-PASER**
100	25	23
200	38	35
300	55	50
400	70	64
500	79	67

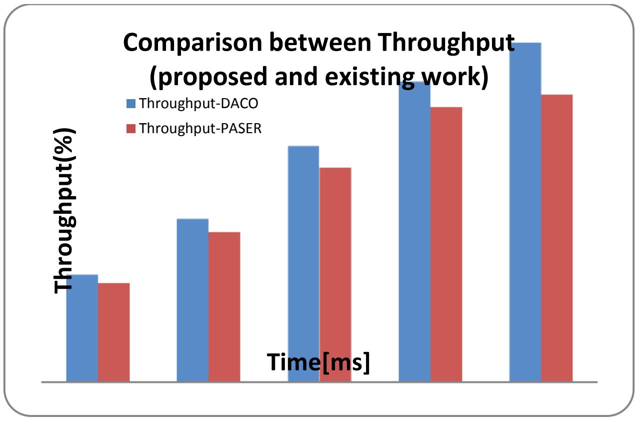

Figure 7 Comparison between throughput (proposed and existing work)

The figure 7 represents that the comparison based on PASER and DACO in throughput (%). We improve the accuracy of the wireless mesh network. We detected and prevention is performed in the network with the help of data ant colony optimization technique and secret key algorithm.

Table 5. Comparison between Packet delivery Rate Proposed and Existing work)

Time [ms]	**Packet delivery rate DACO**	**Packet Delivery Rate PASER**
100	84	54
200	89	58
300	93	60
400	95	69
500	98	70

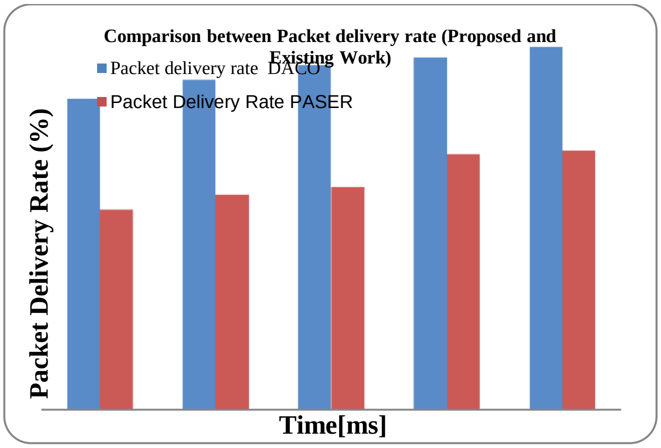

Figure 8 Comparison between PDR (Proposed ad Existing Work)

The figure 8 represents that the comparison based on PASER and DACO in the PDR (%). We improve the packet delivery with DACO and PASER. We implement the proposed approach to enhance the performance of the information transmission.

VII. Conclusion and Future Scope

This paper analyses the DACO secure approach in UAV-WMN. It is concluded that DACO enhance the security and mitigate the attacker effects in the mesh network, secure routing protocol and used the standardized security mechanisms. The efficiency of DACO is explored in a theoretical and simulation based study of its route discovery process, and its scalability with respect to wireless mesh network size and heavy traffic is logical. Using the network simulator MATLAB, accurate mobility patterns of UAVs, and an experimentally derivative channel model of UAV-WMN, it is demonstrated that in UAV-WMN assisted network provisioning and area exploration scenarios PASER have a comparable performance with that of the well-established, non-secure routing protocol HWMP combined with the IEEE 802.11s security mechanisms. Last, the benefits of DACO were recently presented in different events, such as the Vodafone innovation days 2014.

This work can be enhanced in future by using ELGIMAL–AODV protocol in a broader distance of application environment. It will implement the cross-breed approach for improving the performance parameters like network load, packet delivery, throughput or delay.

REFERENCES

[1]. Torjemen, N.,Zhioua, G.S.M., and Tabbane, N., (2015),"A handover decision algorithm from LTE-advanced to Wireless Mesh Network." In *Communications and Networking (COMNET), 2015 5th International Conference on*, pp. 1-6. IEEE.

[2]. S. Mewada, UK. Singh and P. Sharma, "A Novel Security Based Model for Wireless Mesh Networks", International Journal of Scientific Research in Network Security and Communication, Vol.1, Issue.1, pp.11-15, 2013.

[3]. Wu, P., Li, Y., and Liu, X., (2015),"Capacity-based channel assignment scheme in multi-radio multi-channel wireless mesh networks." *Chinese Journal of Electronics* 24, no. 2: 419-425.

[4]. Xing, S., Huang, H., and Wang, R., (2015), "Load balanced coding aware multipath routing for wireless mesh networks." *Chinese Journal of Electronics* 24, no. 1: 8-12.

[5]. Aggeliki, S., and Chatzimisios, P., (2013),"A survey on security and privacy issues in wireless mesh networks." *Security and Communication Networks*.

[6]. Umesh Kumar Singh, Jalaj Patidar , Kailash Chandra Phuleriya, “On Mechanism to Prevent Cooperative Black Hole Attack in Mobile Ad Hoc Networks”, International Journal of Scientific Research in Computer Science and Engineering, Vol.3, Issue.1, pp.11-15, 2015.

[7]. Kato, N., Nishigama,H., and Miura, R., (2015),"Toward fair maximization of energy efficiency in multiple us-aided networks: a game-theoretic methodology." *IEEE Transactions on Wireless Communications* 14, no. 1 305-316.

[8]. Moh, A.N.A., and Borhanuddin, M.,(2015),"Optimum QoS resource allocation algorithm for video traffic over wireless mesh networks based on IEEE 802.11 s." In *Communications (MICC), 2015 IEEE 12th Malaysia International Conference on*, pp. 102-106. IEEE.

[9]. Wang, j., and Lu, k., (2016),"ULNC: An Untraceable Linear Network Coding Mechanism for Mobile Devices in Wireless Mesh Networks." *IEEE Transactions on Vehicular Technology* 65, no. 9: 7621-7633.

[10]. Sbeiti, M., Goddemeier, N., and Wietfeld, C., (2016),"PASER: Secure and Efficient Routing Approach for Airborne Mesh Networks" *IEEE Transactions on Wireless Communications* 15, no. 3 : 1950-1964.

[11]. Akilarasu,G., and Shalinie, S.M., (2016),"Worm hole free routing and DoS attack defense in wireless mesh networks." *Wireless Networks*: 1-10.

[12]. Mayuri, A.V.R., and Subramanyam, M.V., (2015),"MPGA: QOS adequacy latitude aware cooperative spectrum sensing in Cognitive Wireless Mesh Networks by Meticulous Progression based GA." In *Power, Control, Communication and Computational Technologies for Sustainable Growth (PCCCTSG), Conference on*, pp. 318-325. IEEE.

[13]. Akyildiz, I.F., and Wang, X., (2005),"A survey on wireless mesh networks." *IEEE Communications magazine* 43, no. 9: S23-S30.

[14]. Neeraj Paliwal , "Relevance Multipath Forwarding in Intended Wireless Mesh Networks", International Journal of Scientific Research in Computer Science and Engineering, Vol.3, Issue.2, pp.5-10, 2015

[15]. Soufiane, J., Haqiq, A., and Nassereddin, B., (2015),"Fairness and differentiation of services in wireless mesh network." In *Information and Communication Technologies (WICT), 2015 5th World Congress on*, pp. 59-66. IEEE.

[16]. Islam, M.J., Nurain,N., and Raghunathan, V., (2016),"Channel Assignment Techniques for Multi-Radio Wireless Mesh Networks: A Survey." *IEEE Communications Surveys & Tutorials* 18, no. 2: 988-1017.

[17]. Wang, X., Zhang, j., and Zhang, X., (2015),"Monitor Node Selection Algorithm Based on Mutual Information in Wireless Mesh Networks." In *Smart City/Social Com/Sustain Com (Smart City), 2015 IEEE International Conference on*, pp. 349-353. IEEE.