# Design and Development of Fuzzy Means cluster-based Social spider Elliptic Curve Cryptography Routing (FSER) and Comparing the QOS Parameters with AODV Routing Protocol in MANET

[1]B. Sunil Srinivas, [2]Vangala Konica Nehal
[1]Assistant Professor, [2]M. Tech Scholar,
[1,2]Department of Computer Science and Engineering,
[1]TKR College of Engineering and Technology, Hyderabad, India

***Abstract:*** Mobile Ad-hoc Network (MANET) is a kind of independent and self-configuring environment connected by wireless links. Free-Space-Optical (FSO) MANET is one of the recent technologies. The main aim of project is to develop Fuzzy means cluster-based Social spider Elliptic Curve Cryptography Routing (FSER) protocol for the enhancement of security and to prevent the loss of information during routing in FSO MANET. The proposed Method is based on three stages: (i) Cluster formation stage, (ii) Network routing stage and (iii) Secure communication stage. In this paper, the higher demands on growing application can be supported using FSO which has the advantage of low power consumption and higher bandwidth to support huge number of nodes.

***IndexTerms*** **– Hybrid Fuzzy control, Security, Bandwidth, QoS Constraints, Social Spider Algorithm.**

## I. INTRODUCTION

Free-space-optical (FSO) MANET is a current booming technology. It is a cluster of mobile nodes in a FSO network. FSO network establishment is one of the toughest tasks in mobile networks. In existed routing protocols in mobile ad-hoc network such as AODV, DSDV, ZRP, DSR, SRL, HSR so on cannot be implemented for FSO/RF MANET due to some disjoint properties of free space optical (FSO) and MANET. Some features are accommodating accuracy in routing directionality, information, delay and reduced overhead memory. Wireless ad-hoc network takes multiple paths for data transmission, but it is obvious to select an efficient path for transmission and also provide better security for data. Due to frequent movement and formation of dynamic connections in MANET, it is challenging to maintain security. Hence, many research works are presented for the routing in FSO MANET and concentrated on energy and QoS. Hence to developing a routing strategy along with to enhancing the security is our motivated research area. Our work is aimed to design a Security Aware Routing (QAR) protocol for FSO MANET to enhance the security and prevent the loss of data. The proposed work is also concentrated on protocol characteristics to improve all possible parameters like end-to-end delay, throughput, Transmit Energy, channel load, buffer occupancy and bit error rate (BER) to enhance the security while routing in FSO MANET. Thus, the proposed security aware routing protocol for FSO MANET provides better Quality of Service.

## II. LITERATURE SURVEY

[1] Sd.Shabana et.al., Author developed application system which works on three different sections. Those are 1. Formation of clusters 2. Establishing a Routing in FSO MANET 3. Secured data transfer in communication. For the purpose of the formation of clusters, FCM methods are used to form the clusters in FSO MANET, after formation of clusters, efficient routing is established by SSA, through vibrations formed the shortest path in the network among source node and destination nodes. During transformation ECC is included for data transmission and security through encryption and decryption methods. The proposed methodology forms a complete FSER protocol. FSER provides more security and avoids data loss by considering different QOS.

**[**2] K. Naga Divya et.al., This work mainly focused on intra cluster routing including MST (minimum-spanning-tree) algorithm to approximate the least energy consumption case. Later constructing SPT (Spanning-tree), every L-sensor node sends sensor information to H-sensor (Cluster-head) with in a cluster. Proposed methodology presents a preventive technique to overcome non-differential side channel attacks in HSN by enhancing Elliptic Curve Cryptography and it minimizes storage space requirement, communication overhead and energy consumption in HSN.

[3] V. Shanmukha Rao et.al., The main purpose of this proposed technique is to optimize the QoS parameters and security to the network nodes during the route discovery. Here, the work is carried out in the MatLab platform and the analyzed results are compared along with existing protocol like FSER and ANT-DSR in terms of QoS constraints such as PDR, route throughput, route latency, route delay and even route overhead. Hence, the proposed PACR protocol showed it is a least possible method in secure the free space optical mobile adhoc network for quality of service constrains.
[4] Bandani Anil Kumar et.al., This paper makes use of an energy consumption method incorporate with a proactive MANET routing protocol. The routing protocol rely on the energy level and the movement of the nodes. Estimation of energy cost is performed based on the calculation of the energy consumption level of the node, using K-Means clustering along with AODV (Ad-hoc On-demand-Distance-Vector) optimized with Ant Colony Optimization (ACO). The performance of the proposed "K-

Means-AODV-ACO" model is compared with the existing Energy Efficient Hybrid Routing Protocol (EE-HRP) and Mobile Agents based Reliable and energy efficient routing protocol (MAREERP) MANETs.

[5] V. Shanmukha Rao et.al., In this paper, the higher demands on growing application can be supported using FSO which has the advantage of low power consumption and higher bandwidth to support huge number of nodes. First, a temporary topology is created by forming clusters with cluster head in order to consume the energy in which each node having multiple transceivers. Then a quality aware routing is performed by checking the path for QoS demand from source to destination. A secure data delivery from source to destination is provided by encrypting the packets using the ECC authentication scheme.

[6] Vahid Rahmati et.al., A novel PID Controller (PIDC) for the purpose of adjusting an antenna in 360 degrees range by direct current (DC) motors using Fuzzy method is designed and simulated. **Methods:** For this, first, an accurate model for DC motor in simulations is developed- that can be replaced by any other dynamic, for e.g., a high-power low speed motor, however, the response in this case will be different. The controller mentioned uses the Mamdani type in two working modes with 3 and 4 inputs setting the full control of two independent DC Motors (DCMs). **Findings:** Clearly, the modes with 3 and 4 inputs occupy 27 and 81 commands respectively to have smooth overshoot and under shoot responses.

[7] Ashraf Abu-Ein et.al.,In this paper, a new routing protocol for Mobile Ad-Hoc networks (MANETs) is presented; the proposed power-hop based Ad-hoc on demand Distance Vector (AODV) is named PH-AODV, it uses the node power and the hop count parameters to select the best routing path. This paper compares the performance of the proposed PH-AODV in terms of average delay, average dropped packets and average throughput. Results reveal that PH-AODV is much better than AODV.

[8] Mohammed N. Abdullah., The paper proposes an algorithm for intelligent cluster head (CH) election in clustered-AODV-based routing. Initially, the K-mean for clustering the MANET nodes have been used according to their distances between them. Next, the intelligent CH election using soft computing techniques that includes sequential hybrid Fuzzy-Genetic controller for this decision making have also been applied. The paper simulation shows that the clustered–AODV-based routing protocol can be modified by changing the ordinary known AODV protocol (Classical AODV) to comply with the clustered network.

## III. PROPOSED METHODOLOGY

The proposed FSER (Fuzzy C-Means cluster-based Social Spider Elliptic Curve Cryptography Routing) protocol scheme is based upon three phases (a) Cluster Formation (b) Network routing (c) Secure communication phase. During initial phase, the nodes having similar characteristics are grouped into clusters with cluster head. Routing process is performed on the clusters of network with QoS constraints in the second phase. Finally, during routing a secure communication is carried out in the third phase. The proposed diagram shows the process flow of the suggested system (FSER protocol) in which every node develops a routing table that contains ID of the neighboring nodes and QoS status. At the outset, a hello message is sent to all of the nodes associated with the source node. The process flow of the proposed FSER protocol as illustrated in below Fig.1.

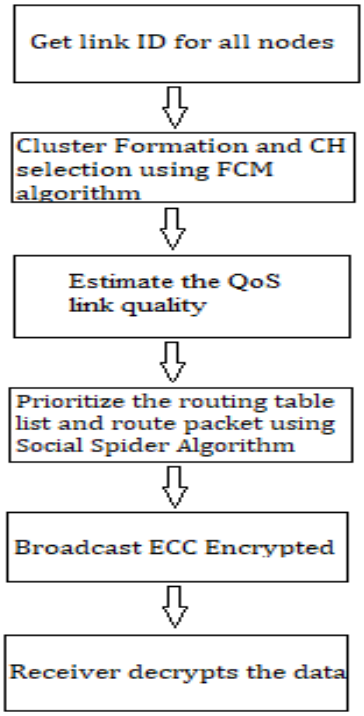


**Fig.1. Work Flow**

### 3.1 Cluster Formation Phase

In this phase, the energy consumption of the network is done by the clustering of nodes at each time during the transmission process will be taken out iteratively. In this paper FCM can be used to do the iterative operation. Fuzzy c-means (FCM) algorithm can be a very convenient process for investigating mobile networks. This clustering process involved in this work in order to group the mobile nodes as hierarchical networks with Cluster head. The clustering of nodes with FSO transceivers is carried out based on the distance between the nodes; if the distance between the nodes is nearer with low energy will be grouped in the similar cluster. In the first part, Fuzzy c-means (FCM) clustering algorithm is employed to form clusters in FSO MANET. In this algorithm, the clustering of nodes are based up on the distance using Euclidean distance as the objective function.

**3.2 Pseudo code for FCM algorithm:**

The algorithm contains the following steps:

1. Arbitrarily chose cluster center
2. Initialize $U = U_{xy}$ matrix, $U^{(0)}$

Determine $U_{xy}$

3. at k-step: find the centers vectors $C_{(k)} = C_{[j]}$ with $U^{(k)}$
4. Modify $U^{(k)}$, $U^{(k+1)}$
5. If $\|U^{(k+1)} - U^{(k)}\| < €$

At that point STOP; or else return to step 2.

The resultant of the FCM algorithm will create the number of clusters with cluster head. These clusters with the highest values are given as inputs to the routing algorithm.

**3.3 Network Routing Phase**

In the second phase, Social Spider Algorithm (SSA) is used to create the routing table through the vibration to other spiders based on the distance of the members and for efficient routing. The transmission process will begin, while the transmission of all possible paths with fewer QoS constraints will be generated through the cluster head or base node. Then from the available paths one of the congestion free with minimum QoS constraints and short distance will be preferred for the routing. Then if any of the nodes left its position means, one of the adjacent nodes to the previous node will be selected based on the trust's ability and distance.

SSA imitates are the powerful character of spiders to execute optimization done the search area29. The search distance of SSA is developed in the system of network where every location is connected with possible clarification of the difficult then boundary to the fitness rate of the impartial function. Spiders apply their movement to work out the location of target and as a protecting notice procedure for themselves. The standard resolution (fitness) of the complication of the food source is detected at the corresponding location. The movement is transferred through the network once the spider's transfer to an oval place and different spiders will be intellect it, this often collaborated with common information is shared among them.

The functioning of SSA is categorized into three stages: initialization, iteration and ending. In every single pass of SSA, it begins with the initialization stage, then examination is activated in an iterative way and the procedure in-depth after finishing all circumstances are matched at the final stage. The flow chart for the procedure of social spider algorithmic rule for effective routing is given in the SSA flow diagram is given below.

***Stage 1: Fuzzy c-means cluster based***

- Cluster formation stage.
- This algorithm works by assigning membership to each data point corresponding to each cluster center on the basis of distance between the cluster center and the data point.
- More the data is near to the cluster center more is its membership towards the particular cluster center.
- After each iteration membership and cluster centers are updated.

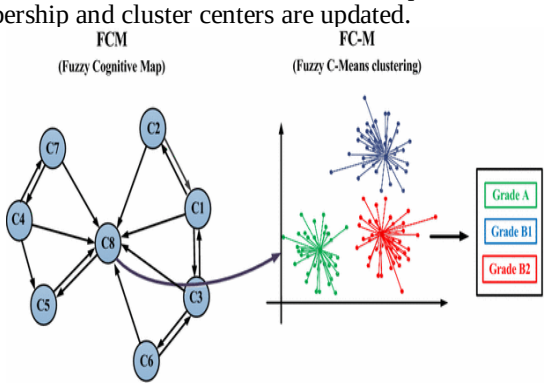


**Fig.2. Cluster Formation Stage**

**Stage 2: Social spider algorithm**

- Network routing stage.
- Social Spider Algorithm (SSA) is used to create the routing table through the vibration to other spiders based on the distance of the members and for efficient routing.
- The transmission process will begin, while the transmission of all possible paths with fewer QoS constraints will be generated through the cluster head or base node.
- Then from the available paths one of the congestion free with minimum QoS constraints and short distance will be preferred for the routing.
- Then if any of the nodes left its position means, one of the adjacent nodes to the previous node will be selected based on the trust's ability and distance.

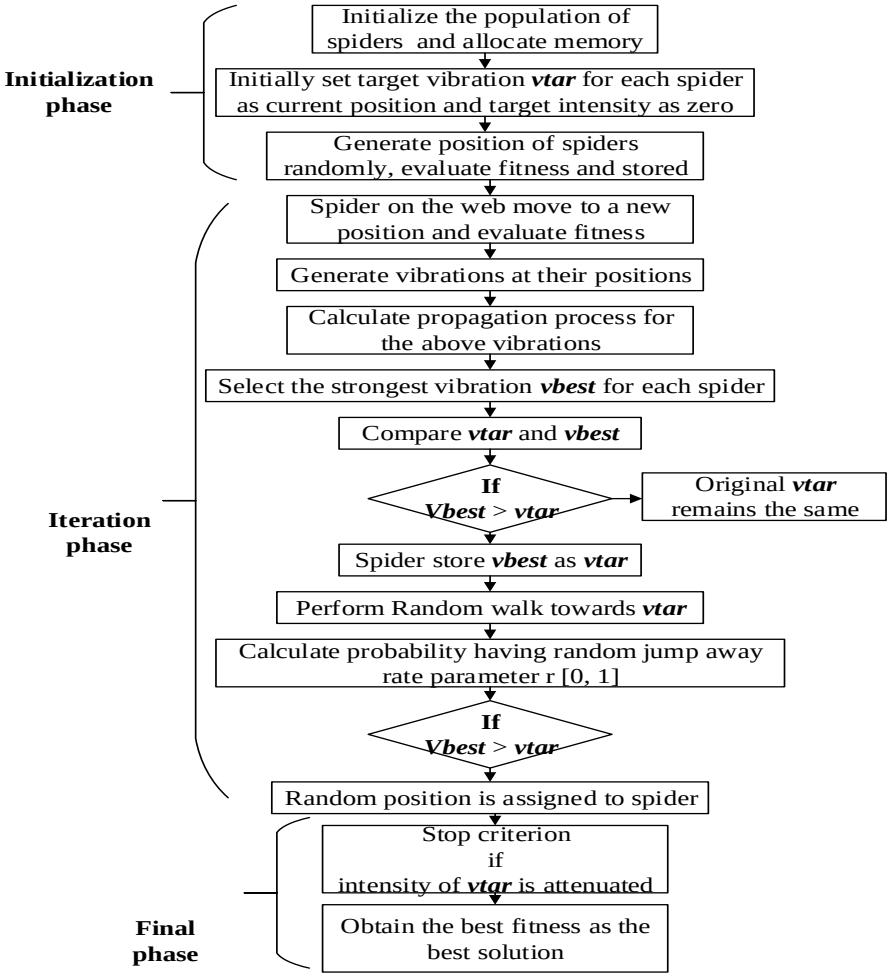


**Fig.3. Social Spider Algorithm**

**Stage 3: Elliptic curve cryptography**

- Secure communication stage.
- It provides secure data delivery from source to destination.
- This phase can be classified into two phases.
- The initial phase is the key selection, which is accomplished ahead of organization of sensor nodes.
- The second phase involves two sub phases. One is the encryption of the data packet before transmission by the sender and the other one is to decrypt the packet by the receiver using private keys which are executed subsequently to position the sensor nodes.

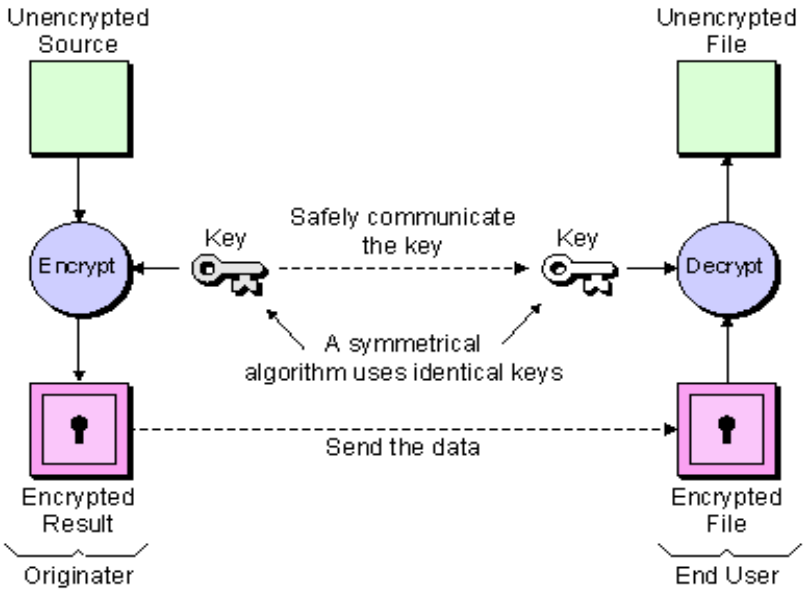


**Fig.4. Encryption and Decryption process**

### 3.4 Secured Communication Phase

In military applications, security of communication in MANETs is very important. Numerous symmetric and asymmetric cryptographic algorithms are developed but it has the difficulty of factoring large integers. In our proposed protocol, the ECC cryptographic algorithm is used for secure communication from source to destination in the FSO MANET. This phase can be classified into two phases. The initial phase is the key selection, which is accomplished ahead of organization of sensor nodes. The second phase involves two sub phases. One is the encryption of the data packet before transmission by the sender and the other one is to decrypt the

packet by the receiver using private keys which are executed subsequently to position the sensor nodes. So that, we propose Elliptic curve cryptography (ECC) for FSO MANET to provide secure data delivery between source and destination.

## IV. PERFORMANCE MATRIX

Some of the important performance parameters responsible for finding the algorithm effectiveness to the universal presentation of the network system in FSO mobile ad-hoc networks are as follows:

### 4.1 Average End to End Delay (AEED)

An enactment of the web in transmitting packets from source to destination is that the delay in getting packets. End-to-end delay is denoted as the period reserved for a packet to be transferred between networks from sender to receiver. The average end- to-end packet delay is measured because the part of total end-to-end delays within the entire communication once related to the quantity of packets will offer to the receiver end nodes throughout the whole recursive run. A low price of this end-to-end delay means that MANET is smaller amounts crowed and accordingly observes the success of proposed routing algorithm.

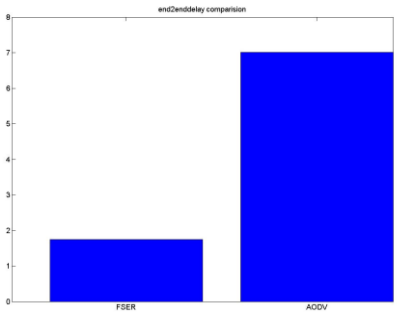


**Fig.5. E-to-E Delay performance comparison**

### 4.2 Average Packet Delivery Ratio (APDR)

It is the proportion of packets received with success to the whole variety of packets transferred with n number of nodes.

$$APDR = \sum_{i=0}^{n} \frac{Packet\ Delivered}{Time}$$

The proportion information gives the instruction about how explicitly the packets in the protocol fetched to the receiving end. The highest value of this ratio represents the better standard of the proposed algorithm's presentation and also committed that more amounts of packets are delivered to the higher layers.

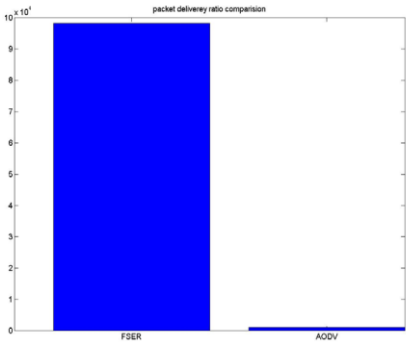


**Fig. 6. Packet delivery Ration comparison**

### 4.3 Average Packet Loss Ratio (APLR)

It is defined as the proportion of packet lost to the total packet send.

$$APLR = \sum_{i=0}^{n} \frac{Packet\ Lost}{Time}$$

The Performance comparison for Packet lost Ratio simulation result obtained as follows.

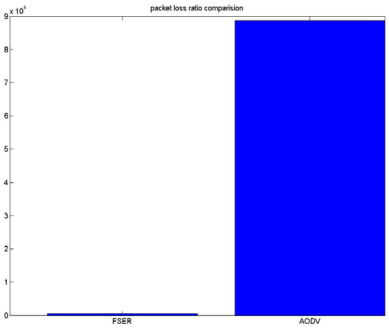


**Fig. 7. Packet Loss Ratio comparison**

### 4.4 Average Delay (AD)

It is demarcated as the time variance among the present packets received and the previous packet received. It is the quantity of packets distributed throughout the data communication.

$$AD = \sum_{i=0}^{n} \frac{packets\ received\ time - packets\ send\ time}{n}$$

The Performance comparison for average delay simulation result obtained as follows.

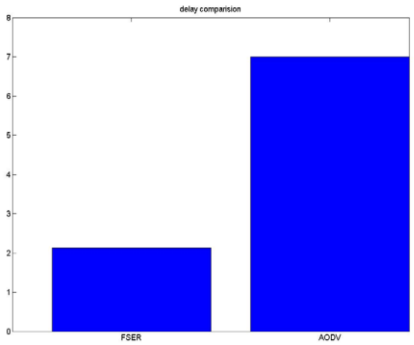


**Fig. 8. Average Delay comparison**

### 4.5 Average Throughput (AT)

Average Throughput is defined as the rate at data is totally transmitted for every packet sent. It is the whole range of packets delivered by the receiver.

$$AD = \sum_{i=0}^{n} \frac{packets\ received * 8}{delay}$$

The Performance comparison for throughput simulation result obtained as follows.

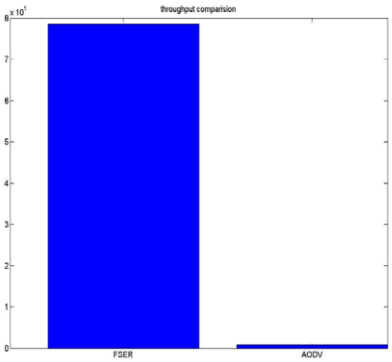


**Fig. 9. Throughput Comparison**

Subsequent to the numerical evaluation performed using the optimization methods, the succeeding statements are made with regard to the results differentiating packet delivery ratio, packet loss ratio, throughput, delay, and average end to end delay. Obtained performances of the proposed FSER protocol in free location optical mobile ad-hoc networks are displayed as graphs that can be compared with existing AODV protocol. This is the result of AODV32 must find the route to retransmit data packets that are misplaced due to the node's flexibility or fanciful route methods during the transmission. The product displays that values of the proposed FSER protocol are much better than AODV protocol. The advantage of FSER established from determining factor the correct routing path or changes the notional route methods simply in time by the reliability of the appropriate QoS metrics.

## V. CONCLUSION

An efficient and secured FSER routing protocol for FSO MANET is proposed. FSO is included for its high bandwidth to bridge the capacity gap among mobile ad-hoc links and fiber links. Our system makes use of Fuzzy C-means clustering around an algorithmic rule to form the cluster inside the cluster head and Elliptic curve cryptography for secured communication of data from source to destination via social spider optimization-based routing. Each node in the network gathers data from whole cluster followers with the help of CH and builds a routing table using the SSRA (Social spider Routing Algorithm). The proposed approach is implemented in MATLAB with enhanced QoS performance metrics in terms of the delay, throughput, packet loss ratio, end-to-end over-all delay, packet delivery compared with the AODV routing protocol.

## REFERENCES

[1] Sd.Shabana, V.Lakshmi Sailaja, S.Keerthana, V.Shanmukha Rao "Developing an FSO MANET Application using FSER Protocol",International Journal for Modern Trends in Science and Technology Volume: 03, Special Issue No: 02, March 2017 ISSN: 2455-3778 http://www.ijmtst.com.

[2] K. Naga Divya, D. Sree Lakshmi, K.Sri Vijaya "A Routing-Driven elliptic Curve cryptography Based Key Management Scheme for Heterogeneous Sensor Networks", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X,Volume 2, Issue 9, September 2012.

[3] V. Shanmukha Rao, V. Srinivasa Rao "Implementation and Comparative Study of Pillar K-Means Ant lion Caesar Cipher Routing Protocol (PACR) with FSER Protocol in FSO MANET", International Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801
ISSN (Print): 2320-9798, Vol. 5, Issue 1, January 2017, www.ijircce.com.
[4] Bandani Anil Kumar, Makam Venkata Subramanyam, Kodati Satya Prasad "An Energy Efficient Clustering Using K-Means and AODV Routing Protocol in Ad-hoc Networks", International Journal of Intelligent Engineering & Systems, November 15,2018.
[5] V. Shanmukha Rao, V. Srinivasa Rao "Security Aware Fuzzy C-Means Cluster-based Social Spider Elliptic Curve Cryptography (FSER) Routing Protocol in FSO MANET", Indian Journal of Science and Technology, Vol 9(44), DOI: 10.17485/ijst/2016/v9i44/98473, November 2016.
[6] Vahid Rahmati, Amir Ghorbani "A Novel Low Complexity Fast Response Time Fuzzy
PID Controller for Antenna Adjusting Using Two Direct Current Motors",Indian Journal of Science and Technology, Vol 11(13), DOI: 10.17485/ijst/2018/v11i13/113270, April 2018.
[7] Ashraf Abu-Ein, Jihad Nader "An enhanced AODV routing protocol for MANETs", IJCSI International Journal of Computer Science Issues, Vol. 11, Issue 1, No 1, January 2014.
[8] Mohammed N. Abdullah, Mahmood Zaki Abdullah, Rooa Adnan Sabri "AODV Protocol Improvement using Intelligent Clustering", International Journal of Computer Applications (0975 – 8887), Volume 88 – No.7, February 2014.