Indian Journal of Science and Technology, *Vol 9(44), DOI: 10.17485/ijst/2016/v9i44/98473, November 2016*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Security Aware Fuzzy C-Means Cluster-based Social Spider Elliptic Curve Cryptography (FSER) Routing Protocol in FSO MANET

V. Shanmukha Rao[1*] and V. Srinivasa Rao[2]

[1]Department of Information Technology, Andhra Loyola Institute of Engineering and Technology, Vijayawada - 520008, Andhra Pradesh, India; shanmukharao.v@andhraloyola.org, shanmukharao.v@gmail.com
[2]Department of Computer Science Engineering, V.R. Siddhartha Engineering College, Vijayawada - 520007, Andhra Pradesh, India; drvsrao9@gmail.com

Abstract

Objective: To design an FSER (Fuzzy _means cluster-based Social spider Elliptic Curve Cryptography Routing) protocol to enhance the security and prevent the loss of data while routing in FSO MANET. **Methods/Statistical Analysis:** Our proposed protocol scheme is based on three stages: (i) Cluster formation stage, (ii) Network routing stage and (iii) Secure communication stage. In the first stage, an efficient Fuzzy c-means (FCM) clustering process is used to form clusters in FSO MANET. In the second stage, Social Spider Algorithm (SSA) is used to create the routing table through vibration to other spiders based on the distance from the members and efficient routing through vibration intensity of spiders in the web. In the third phase, we suggest an Elliptic Curve Cryptography (ECC) Algorithm for MANET to provide secure data delivery from source to destination. **Findings:** A hierarchal secure FSER routing protocol for FSO MANET is proposed. Nowadays, MANETs are demanding higher bandwidths, smarter and faster. 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. **Improvements/Application:** Experimental simulations on FSO MANETs are implemented in MATLAB tool by finding an optimal path to demonstrate the effectiveness of the proposed FSER protocol that fulfills several Quality of Service (QoS) constraints. The designed proposed protocol in FSO is observed to be performing well with high speed optical modulation for bandwidth intensive applications like multimedia.

Keywords: Elliptic Curve Cryptography, Fuzzy C-Means, Free-Spaceoptical, Security, Social Spider Algorithm

1. Introduction

Mobile ad hoc network (MANET) is an autonomous and self-configuring system connected by wireless links. Free-space-optical (FSO) MANET is a recent technology. It is a collection of mobile nodes in a FSO network. FSO network establishment is a challenging in mobile networks. The existing routing protocols in mobile ad hoc network such as DSDV, AODV, DSR, ZRP, SRL, HSR, etc cannot be utilized for FSO/RF MANET owing to certain disjoint characteristics of free space optical (FSO) and MANET. The characteristics are accommodating directionality, accuracy in routing information, memory, reduced overhead and delay. Wireless ad hoc network uses multiple paths for data transmission, but it is necessary to choose most efficient path for transmission and also

*Author for correspondence

provide better security for data. Due to frequent movement and formation of dynamic connections in MANET, it is challenging to maintain security. So far 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. Moreover the proposed security aware routing protocol for FSO MANET provides better Quality of Service.

2. Literature Review

Free-Space Optical (FSO) is a wireless point to point communication system with high speed internet accessibility for mobile ad hoc networks. Of late, it has become critical to improve FSO presentation in a range of framework, with many powerful technological and elementary challenges[1]. Historically, RF MANET is performed various investigations have been carried out in discovering guiding system of RF Antennas for attaining enhanced robustness in network to maintain higher amount of nodes[2]. The high mobility protocols are reported with FSO for some primary construction blocks for high speed mobile ad hoc networks (MANET[3]). Free space optical transmission with associate advanced multi section node structure will impact spatially varied optical wireless connections. There is a need to create feasible solution to the recognized reduction per node throughput in large measure of RF networks[4].

Now the foremost concentration in the network towards routing protocols designed for routing proficiency trend towards different attacks in Mobile Ad-Hoc Networks (MANET[5]). The transmitting procedure for analysis of malicious nodes and assortment of maximum protected, absolute, near a trustworthy and the shortest path for transmitting the knowledge packets in mobile circumstantial systems is developed[6]. FSO topology conveys complete movement of the set-up during transmission. Hierarchical state routing protocol is mainly used for solving the routing difficulties in RF ad-hoc fields. It depends on logical and cluster sub network[7].

In the field of mobile ad hoc networks (MANET), Arrange the minimum amount of movable packets, effectively refine the delay, throughput, and security presentation[8]. It is exacting to find the optimal position of mobile transfer in such hybrid MANET[9]. Mobile ad hoc networks could be making as an assortment of post-disaster situations, allowing initial-acceptor for prioritizing the usage of benevolent in analytical position initiated through great meteorological conditions such as hurricanes, shakings, torrents, and snowflake[10]. The sender and receiver of ORRP send path position and path movement packets correspondingly in locally selected orthogonal regulations.

A lightweight but accessible transmitting orthogonal rendezvous routing protocol (ORRP) applying multi directional transmission like free-space-optical transceivers or reversing antennas to modify data wants like correlate house embedding and node variation[11]. Advanced stratum routing procedures might not be continuously identifying the identical route as calculated by means of enhanced physical layer instigating argument plus dissention[12]. A certain level of QoS framework like bandwidth, delay, packet transportation ratio and throughput should be produced by the routing protocols[13] so that the objective is accomplished. The security resolution must deliver whole reassurance intersection, the whole protocol stacks[14].

In MANETs, this is remarkably true given the minimum physical security of mobile devices. Multi-level security procedure is required in wired networks from the design of security[15]. In mobile ad hoc networks (MANETs), associate elementary involves presentation regarding to the transmission between nodes that nodes ought to establish by one another[16]. Real-time information distributing the data, using a mobile app, has been spread out from 'hot-spots' to 'dynamically construct' or 'the single point-to-point communication', with virtual hub-and-spoke topology, mobile ad hoc networks[17]

An effective and constructive AMDMM methodology (Audit Misbehavior Detection and Monitoring Method), which meritoriously detect mutually critical and constant packet dispensers to transmit the packets via the presumed nodes[18]. Communication has been taken united of the possible results for the response to the always increasing wireless largeness request in Free-space-optical (FSO), a.k.a. optical wireless network[19]. Routing protocols should be extremely powerful and consistent to ensure eminent packet transference once the nodes transfer arbitrarily.

Mobile improvised Networks (MANETs) performance is an absolute role in substitute transmission anywhere network must be recognized quickly and temporarily[20]. By reason of the important stimulus of impressive belongings and the substances respective motion, pointing and tracking(APT), accession remain the crucial skills for constructing the transmission relationship in free space optical communication[21].

Routing procedures should be extremely powerful and dependable to assurance effective packet transportation when the nodes move randomly. Mobile Ad hoc Networks (MANETs) show the complete part in place of alternative transmission wherever a system wants to be established rapidly and provisionally[22].

The recent related work associated to the MANET routing protocol[23] as follows:-

An authoritative way of MANETs includes the consumption of routing protocols to get extraordinary implementation in the administration's maintenance by the system; greatly additional administrations present extreme religious requirements, for example, vision and sound or VoIP administrations. MANETs are experiencing constant progress because of their decentralized topology and their simple and ease arrangement. A unique routing procedure for important exploration application was excited in the BATMAN procedure that suggests standard keeping away from the unambiguous skills of routing data among nodes[24]. Concentrate on an estimate the execution of BATMAN associating VoIP programmed on small power-consumption protuberances, commencing a Quality of Experience (QoE) location. In specific, they measure the result on BATMAN execution of 1) the physical layer, through exploiting a dissolve explanation of the communication passage; 2) the quantity then solidity of ad-hoc nodes; and 3) node superiority. Entirely outcome acquired for BATMAN was associated, and people acquired via applying the generally applied OLSR routing procedure. Beginning the outcomes, they assume that neither BATMAN nor OLSR in their separate present convention was sufficiently appropriate for VoIP movement support in MANETs made out of animation economical nodes.

In MANET,[25] have proposed effective power aware routing (EPAR), another control conscious directing rules that build the network period of MANET. In contrast to standard power responsive algorithms, EPAR received the range of a node by its leftover power control, as well as by the normal animation expended in dependably sending information packets over a specific connection. Without a doubt, our proposed plan decrease for more than 20 % the cluster animation utilization then reduces the mean particularly for great weight networks whereas managed a respectable packet transport proportion. Utilizing a mini max construction, EPAR selects the way that had the highest packet limit by the side with the minimum wanted packet communication limit. This procedure should have the proficiency to carry high skillfulness of the nodes that frequently give birth to changes within the system procedure.

Numerous individual increased systems are planned seeable of packet encryption to secure the correlation obscurity of versatile especially allotted systems (MANETs).[26] have approved that MANETs were static and ineffective under passive arithmetical traffic investigation strike. To show, how to control the correspondence design without unscrambling the fixed packets, they presented an original numerical traffic configuration detection system (STARS). STARS operate passively to widespread traffic exploration in light of numerical attributes of fixed unrefined traffic. STARS were fit for finding the sender, the receiver, and the end-to-end correspondence relationships. Advanced trainings show that STARS implement great exactness in the secreted transportation designs.

The spread code is critical to set up before the carrying parties explicitly find each other. While rich activity, of late, proposed to break this circular reliance, the interesting components of adjacent disclosure in MANETs make them not straightforwardly pertinent to. Secure neighbor report is fundamental to mobile ad hoc networks (MANETs) conveyed in minatory situations and suggests to the procedure in which two neighboring hubs trade messages to find and authenticate each other. It is vulnerable to the jamming assault in which the opponent intentionally transmits radio signs to prevent neighboring hubs from trading messages. Hostile to jamming communications regularly based on spread-range procedures, which rely upon a spreading code basic to the communicate parties, unclear to the jammer[27] have proposed JR-SND, a jamming-flexible secure neighbor disclosure plan for MANETs in view of direct sequence spread spectrum and unusual spread-code pre-distribution. JR-SND authorized neighboring nodes to identify each other with overpowering likelihood, the presence of omnipresent jammers. Point by point hypothetical and reproduction results declare the viability and productivity of JR-SND.

The next section of this manuscript is given below. The proposed technique used to secure communication of packet through new protocol is mentioned in section 3. The investigational outcomes and analysis in the consideration are mentioned in section 4. In section 5, the conclusion is given.

3. Proposed Work

The proposed FSER (Fuzzy c_means cluster-based Social Spider Elliptic Curve Cryptography Routing) protocol scheme is based upon three phases: (i) Cluster Formation phase, (ii) Network routing phase and (iii) Secure communication phase. In the first 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 follows. (Figure 1)

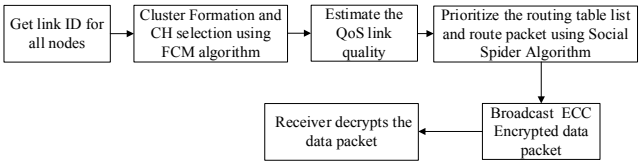

Figure 1. Process flow of the proposed FSER Protocol.

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

This algorithm was established by Dunn and afterwards performed by Bezdek[28]. Fuzzy Theory is the prime abstraction for FCM Clustering algorithm. In the extreme stage of the FCM process, each data point in the set is integrated with all the available clusters with some "degree". This degree is called "membership" to various clusters. The algorithm collects knowledge set having n variety of nodes and created the variety of clusters. Therefore, the data points are present in different multiple groups rather than one. The objective of the FCM is for minimal distance from source to destination can be given as,

$$F(x,y)=\sum_{x=1}^{N}\sum_{y=1}^{C}u_{xy}^{m}\left\|x_x-c_y\right\|,\ 1\le m\le\infty \qquad (1)$$

wherever m (the Fuzziness Exponent) is in reality, bigger than 1, N represents the amount of nodes arrayed in the network, C represent the clusters, u_{xy} is the membership of data point N_y with cluster center C_x, x_x denotes the x^{th} of d-dimensional calculated data, c_y denotes the d-dimensional middle cluster (cluster head), and ||*|| denotes any standard communicate the equivalence among several considered records and center. The objective function is reduced with respect to the Euclidean space between the center of the cluster C_x and the data point N_y. That is, for a given center of the cluster C_x the data points closer to it will have higher membership values. Update the membership u_{xy} in eqn. 6 and cluster centers c_y in eqn. 9 to attain an iterative optimization using fuzzy partitioning for the objective function.

$$u_{xy}=\frac{1}{\sum_{k=1}^{c}\left(\frac{\left\|x_x-c_y\right\|^2}{\left\|x_x-c_k\right\|^2}\right)^{2\times\frac{1}{m-1}}} \qquad (2)$$

Where, $\left\|x_x-c_y\right\|$ is the space from point i to the present cluster center y, $\left\|x_x-c_k\right\|$ is the space from point i to other cluster centers k.

$$\mu_{ij}\in[1,0]\ \ \forall i,j \qquad (3)$$

$$\sum_{i=1}^{C}\mu_{ij}=1\ \forall j \qquad (4)$$

Above Eqn. (8) implies that every data point necessarily belongs to at least one cluster, and hence, is not isolated.

The cluster head of each cluster can be measured as,

$$c_y = \frac{\sum_{x=1}^{N} u_y^m * x_x}{\sum_{x=1}^{N} u_y^m} \quad (5)$$

$$\max\left\{\left|u_{xy}^{k+1} - u_{xy}^{k}\right|\right\} < \varepsilon \quad (6)$$

The repetition will stop when $\max\left\{\left|u_{xy}^{k+1} - u_{xy}^{k}\right|\right\} < \varepsilon$, where ε is an end constraint between 0 and 1; however k is the replication period.

FCM process starts with the initialization of the partition matrix $\mu_y(0)$, at step k the cluster centers are updated using Eqn. 5. $\mu_y(k)$ is updated using Eqn. 2, and the FCM process is repeated until it converges or Eqn. 6 holds.

Pseudo code for FCM algorithm:

The algorithm contains the following steps:

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

Determine u_y from eqn. 2

3. at k-step: find the centers vectors $C^{(k)} = [c_j]$ with $U^{(k)}$
4. Modify $U^{(k)}$, $U^{(k+1)}$
5. If $\left\|U^{(k+1)} - U^{(k)}\right\| < \varepsilon$ or the least $F(x, y)$ is reached,

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.

3.2 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.

The objective function of the proposed system to compute a route from source x to destination z through a neighbor y for QoS aware routing is calculated as:

$$F(x, z) = \alpha D + \beta BW + \gamma H \quad (7)$$

The paper aims at minimizing the objective function subject to several constraints such as Delay D, Bandwidth BW, Hop count H. α , β and γ are the tunable parameters i.e., $\alpha + \beta + \gamma = 1$.

Delay Constraints:-

$$D = delay\{path(x, y)\} = R_t - S_t \quad (8)$$

Where $delay\{path(x, y)\}$ is established as the time variation between the current packet received R_t and the previous packet received S_t.

Bandwidth constraints:-

$$BW = bandwidh\{path(x, y)\} = \frac{P_s}{R_t - S_t} \quad (9)$$

Where $bandwidth\{path(x, y)\}$ is established as the ratio of capacity of the packet P_s to the time difference between the current packet received R_t and the previous packet received S_t.

Hop Count Constraints

$$H = hop\,count\{path(x, y)\} = \frac{R_s - 96}{32} \quad (10)$$

Where R_s is the number of crossed- routers. The hop count calculation specifies the amount of nodes visited by path request message from source x to receiving node y.

SSA imitates are the powerful character of spiders to execute optimization done the search area[29]. 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.

$$f(P_s) = \min(F(x,z)) \quad (11)$$

At the beginning of the algorithmic rule, a pre-established range of spider's area unit position to the random position on the online. Every spider within the search distance constrains the data in its recollection. (i) The specific location of the web; (ii) Fitness of the present location of s and (iii) Objective movement in the previous repetition. The oscillation created by means of spider is well demarcated by two things viz. The property of the oscillation created by the spider is associated to the fitness cost of the location. The source location is the power of oscillation of the source. The source location over the exploration area is outlined through the target operate and therefore the power of oscillation differs within the series [0, +∞].

The position of spider a at time t is demarcated as $P_a(t)$. The power of the oscillation of spider is perceived by spider b at time t is defined as $O(P_a, P_b, T)$ .The oscillation power created by spiders s on the source locality is defined as $O(P_s, P_s, T)$. This is straightly equivalent to the fitness of the source location $f(P_s)$ and is described in Equation 12:

$$O(P_s, P_s, T) = \left(\frac{1}{f(P_s)} - C_{\min}\right) \text{For minimization} \quad (12)$$

Wherever the range of constant $C_{\min}$ is determined it is certainly small among all the functional standards of the reduction is difficult. The equation shield that, the movement concentrations the confident values and assurance the higher fitness values. The oscillation created by spider got reduced over a period of time and distance.

Attenuation over Distance to generate routing table list: $D(P_a, P_b)$ Represent the space among spider 'a'and spider 'b'. The utmost space between two facts is denoted as $D_{\max}$ in the traverse distance and problematic self-governing. In place of perspicuity, Equation 13 is calculated:

$$D_{\max} = \left\| \overline{X} - \underline{X} \right\|_P \quad (13)$$

Everyplace $\overline{X}$ is described as higher inevitable and $\underline{X}$ is the minor inevitable of the pursuit distance. p Represent as p-norm system that is used to evaluate the space. In Equation 14 is estimating the space between spider 'a' and spider 'b'.

$$D(P_a, P_b) = \left\| P_a - P_b \right\|_P \quad (14)$$

In order to evaluate distance during this manuscript, Manhattan norm or 1-Norm is employed. The movement reduction completed space is deliberated in Equation 15:

$$O(P_a, P_b, T) = \exp\left(-\frac{D(P_a, P_b)}{D_{\max} \times r_a}\right) \quad (15)$$

Where r_a the user is measured constraint that manage the reduction amount of distance outlined within the range (0, 1). 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. (Figure 2)

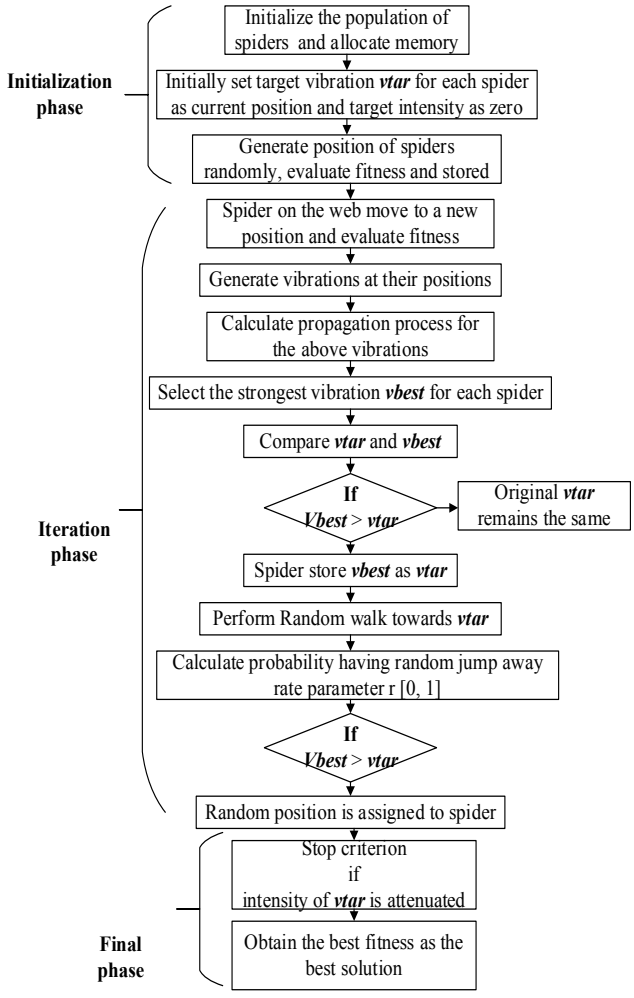

Figure 2. Flow Diagram for Social Spider Algorithm.

Step 1: Initialization phase

In the initialization phase, a fixed memory location is given to each spider to store information, and the spider size must be constant. The positions of spiders are formed randomly within the search area and store the calculated fitness standards. The vibration of every spider is ready at its present location within the population and the vibration power is zero.

Step 2: Iteration phase

In the iteration section, all spiders arranged on the web get a new location and its fitness values are evaluated. The fitness tenets of total replicated spiders remain measured on completely various locations on the net. Every spider can receive totally several vibrations V created by alternative spiders. In the search space, spiders produce oscillation at their locations using Equation 16. The received data involves the source location of the movement and its actual concentration. The sturdiest vibration $vbest$ from V is designated for every spider and balanced its intensity by means of the objective vibration intensity $vtar$ kept in its memory. If the strong point of $vbest$ is further than the $vtar$, then the s will store $vbest$ as $vtar$, or else the inventive value of the $vtar$ remainders equal. At that moment $vtar$ towards spider contrivance arbitrary walk, this arbitrary walk is calculated in Equation 16:

$$P_s(T+1) = (P_{tar} - P_s) \otimes (1 - \beta \otimes \beta) \tag{16}$$

Where $\otimes$ denotes section wise relationship, $P_s(t+1)$ represents the unit of spider s at time $(t+1)$ Afterwards, arbitrary walk and P_{tar} are the oscillation source locations of objective vibration $vtar$. β Represents the direction of arbitrary statistics created starting from zero to one and 1 is a trajectory of ones, whose span is equivalent to the measurement of the target ask. After the random walk step, there is a tiny likelihood to search out whether or not or not the spider monitors its facility objective or jump distant from its present location. The fake spider jump away procedure is believed so those avoid spiders for receiving in specific targets. The probability is calculated in Equation 17:

$$P_j = \frac{r_j}{\exp\left(\frac{D(P_s, P_{tar})}{D_{\max}}\right)} \tag{17}$$

Where r_j denote the worker well-defined jump away amount restriction. If the spider s is decided to leap away, a brand innovative arbitrary location is created and allotted because the new location of s within the exploration area.

Step 3: Final Phase

The final part standards may be defined because the most replication range extended, the highest CPU period, the large amount for the duplication, with not all developments on the initial fitness value, or every proper standard. After the repetition completed, the algorithmic rule yields the best solution. The overhead of three stages encompasses the entire algorithmic rule of SSA. The repetition section can stop once the stopping condition is matched. While routing there may be an intruder to detect the packet, so before routing in this paper, a secure ECC encryption scheme is applied for secured communication.

3.3 Secure 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)[30] for FSO MANET to provide secure data delivery between source and destination.

Step 1: ECC Key Generation Phase

The elliptic curve of the real numbers over field E is represented as $y^2 = x^3 + \boldsymbol{x}^2 + t^2$. Let P is chosen randomly but it must be a prime number. The duplication of roots is avoided if s and t satisfies the condition $4s^3 + 2\,t^2 \neq 0$. The determination of the elements in an elliptic curve over a primary area, the curve equation and the condition changed over as $\left(y^2 = x^3 + sx^2 + t^2\right)_{\mathrm{mod}\,P}$ and $\left(4s^3 + 27t^2\right)_{\mathrm{mod}\,P} \neq 0$.

$$R=\left\{(x,y):\left(y^2=x^3+sx^2+t^2\right)_{\text{mod}\,P}\right\}\cup\{\infty\} \quad (18)$$

An elliptic group $E_P(s,t)$ is formed for quadratic residues $Z_p=1,\cdots p-1$.

There are some of the basic operations that can be used in ECC.

Using the scalar, multiplication can be given hereunder as:

Point Addition

Assume $Z(j_1,k_1)\ W(j_2,k_2)\in R(k)$ and the point on the elliptic curve is E, where $Z\neq W$. Then $Z+W=(j_3,k_3)$

In which $j_3=\left(\frac{k_2-k_1}{j_2-j_1}\right)^2+(-j_1-j_2)$ and $k_3=(j_1-j_3)\left(\frac{k_2-k_1}{j_2-j_1}\right)^2-k_1$

Point Doubling

Assume $Z(j_1,k_1)\in R_Q(s,t)$ and the point on the elliptic curve is E, where $Z\neq -Z$. Then $2Z=(j_3,k_3)$

In which $j_3=\left(\frac{3j_1^2+s}{2k_1}\right)^2-2j_1$ and $k_3=\left(\frac{3j_1^2+s}{2k_1}\right)^2(j_1-j_3)-k_1$

Point Multiplication

Let the spike on the elliptic curve (Z) be Q. Then, the point multiplication of the point Q is denoted as repeated addition. $ZQ=Q+Q+\cdots Z\ times$.

Generating separate public and private keys

If a sender X needs to communicate the message to the receiver Y then they decide upon to use an elliptic curve $E_p(s,t)$ where p is a prime digit and a generator point Z on the elliptic curve. From the range [1, p-1], the sender uses receivers private key α. The sender computes $\beta=\alpha Z$ as their public key. While conveying the message the sender sends the public key along with the cipher text.

Step 2: Encryption Phase

The sender chooses an arbitrary number k and utilizes the receiver's public key to encrypt the plain text fact into the cipher text couple of points.

$$E_p=[(kZ),(m+k\beta)]=[\gamma_1+\gamma_2] \quad (19)$$

In the above equation, E_p is the encrypted plain text point, and m is the message point used for encryption.

Step 3: Decryption Phase

When the receiver receives the cipher text point E_p, receiver uses his private key α to calculate the plain text point m, as follows

$$m=[\gamma_2-\alpha\gamma_1] \quad (20)$$

Finally maps the plain text point m back into the original message. Thus, we can securely communicate from source to destination using Elliptic Curve Cryptography in the FSO MANET.

4. Experimental Results and Discussion

Experimental performance is evaluated in terms of QoS routing and security throughout transmission in FSO MANET. The proposed FSER protocol is simulated using MATLAB R2010b version 7.11.0.584 and the performance are compared with the prevailing AODV (Ad Hoc on Demand Distance Vector) protocol[31].

4.1 Simulation Environment

We discovered the simulation exploration operating MATLAB with a hundred nodes systematically distributed. Each node is equipped with multiple Omni directional RF and FSO transceivers. An arbitrary network location within a neighborhood of 100 X 100 m is taken into account. The nodes are randomly placed at a specific location. To evaluate the presentation of our algorithm, every time a cluster head is recognized using FCM algorithm. The nodes might proceed with overall feasible regulation using supplanting mutable consistently between 0 to a maximum value. In order to have the conventional framework for the FCM, the first one hundred nodes are randomly initialized within the two dimensional distance, clusters c=3, fuzziness exponent m=2, dissolution standard $\varepsilon=1\times10^{-5}$ and iteration =100.Then, the framework for social spider algorithmic rule is initialized as worth of constant $c_{\min}=1$ and user controlled parameter $r_a=0.2$.Finally, the secure communication of data packet through ECC initialized with prime number p=23 and roots of the equation $(s,t)=(1,1)$.Additional simulation factors are considered as parameters are mentioned below. (Table 1)

Table 1. Simulation Parameters

Parameter	Value
No. of nodes	100
Deployment Area	100m×100m
Mac	802.11
Traffic source	CBR
Distance between two adjacent nodes	1-100 m
Propagation Model	Free Space Optical
Antenna Type	FSO/ RF antenna
Sending Rate	1 packet/sec
Packet Size	512 bit

4.2 Performance Metrics

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:

4.2.1 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. The performance comparison for End-to-end delay simulation result obtained as follows. (Figure 3)

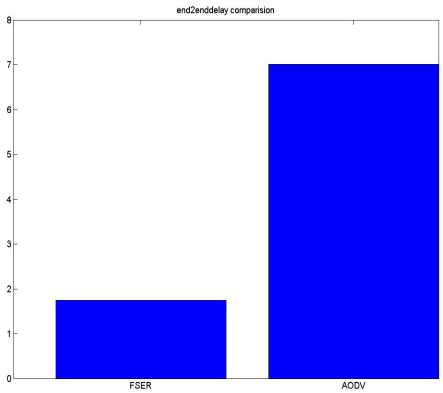

Figure 3. Performance comparison for End-to-End delay.

4.2.2 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.

$$APDR = \frac{\sum_{i=0}^{n} packets\ delivered}{Time} \tag{21}$$

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. The Performance comparison for Packet Delivery Ratio is simulation result obtained as follows. (Figure 4)

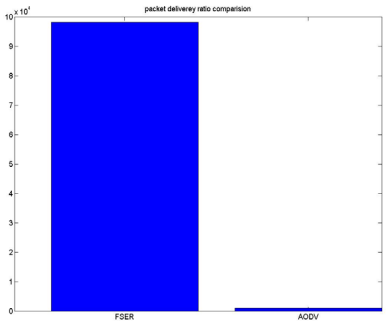

Figure 4. Performance comparison for packet delivery ratio.

4.2.3 Average Packet Loss Ratio (APLR)

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

$$APLR = \frac{\sum_{i=0}^{n} packets\ lost}{Time} \tag{22}$$

The Performance comparison for Packet lost Ratio simulation result obtained as follows. (Figure 5)

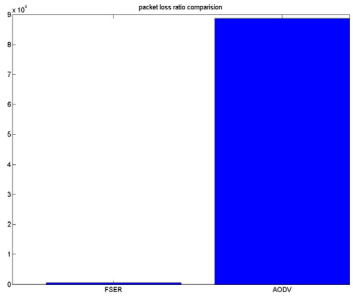

Figure 5. Performance comparison for packet loss ratio.

4.2.4 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.

$$AD = \frac{\sum_{i=0}^{n} (packets\ received\ time - packets\ send\ time)}{n} \quad (23)$$

The Performance comparison for average delay simulation result obtained as follows. (Figure 6)

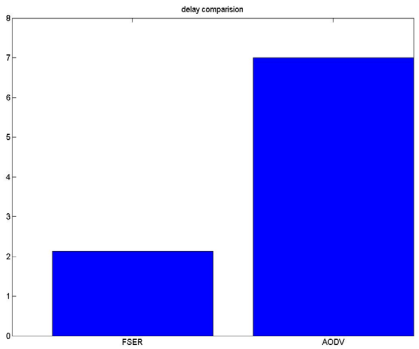

Figure 6. Performance comparison for average delay.

4.2.5 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.

$$AT = \sum_{i=0}^{n} \left(\frac{packets\ received * 8}{delay} \right) \quad (24)$$

The Performance comparison for throughput simulation result obtained as follows. (Figure 7)

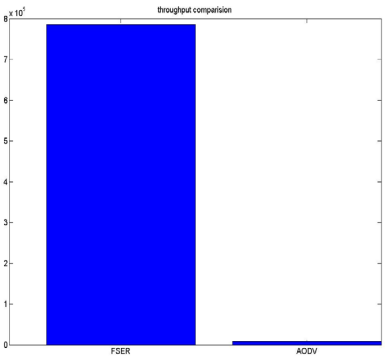

Figure 7. Performance comparison for throughput.

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 AODV[32] 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.

QoS metrics mentioned in table 2 will give the Social Spider Routing Algorithm solutions for the requested QoS relationship from source to destination. The outline of the results is for the track with completely various senders to destination in expression of the QoS metrics throughput and delay.

Table 2. QoS metric measures from source to destination

Source	Destination	Path	Throughput(Mbps)	Delay
1	2	1-70-2	7.7	2
1	5	1-7-5	7.5	1
2	4	2-75-4	7.5	1
2	5	2-80-5	7.7	1
3	4	3-15-4	7.8	2
3	5	3-76-5	8	2
4	7	4-28-7	7.8	1
4	2	4-98-2	7.8	1

5. Conclusion

Secure energy consumed routing in Free Space Optical Mobile Ad hoc Networks is one of the motivated research areas with complex tasks in the field of computer networking. In this paper, a hierarchal secure FSER routing protocol for FSO MANET is proposed. FSO is used due to its high bandwidth to bridge the capacity gap between mobile ad hoc links and back bone fiber links. The proposed system uses the Fuzzy c_means clustering around an algorithmic rule to form the cluster within the cluster head and Elliptic curve cryptography for secure

communication of data from source to destination through social spider optimization based routing. Every node on the network collects information intended for entire cluster supporters with the help of CH and constructs a routing table using the Social Spider Optimization Algorithm. Once the source node of a web desire towards direct information then proposed FSO/RF MANET routing protocol is employed to receiver node on the network. The proposed protocol is implemented in MATLAB tool with improved QoS performance metrics in terms of the end-to-end delay, over-all delay, throughput, packet loss ratio, packet delivery compared with the AODV routing protocol.

6. References

1. Arun K, Majumdar M. Fundamentals of Free-Space Optical (FSO) Communication System, Advanced Free Space Optics (FSO), Springer New York. 2015; 186:1–20.
2. Devi S, Sarje A. Dir-DREAM: Geographical Routing Protocol for FSO MANET. Intelligent Distributed Computing, Springer International Publishing. 2015; 321:95–106.
3. Arun K, Majumdar M. Free-space Optical (FSO) Platforms: Unmanned Aerial Vehicle (UAV) and Mobile, Advanced Free Space Optics (FSO), Springer New York. 2015; 186:203–25.
4. Bilgi M, Yuksel M. Capacity scaling in free-space-optical mobile ad hoc networks, Elsevier, Ad Hoc Networks. 2014; 12:150–64.
5. Schweitzer N, Stulman A, Shabtai A, Margalit RD. Mitigating Denial of Service Attacks in OLSR Protocol Using Fictitious Nodes. IEEE Transactions on 15, Mobile Computing. 2016; 1:163–72.
6. Korea D, Dhurandher SK, Reddy BVR. Enhancing the Security of Dynamic Source Routing Protocol Using Energy Aware and Distributed Trust Mechanism in MANETs. Springer International Publishing on Intelligent Distributed Computing. 2015; 321:83–94.
7. Kumar DK, Murthy YSSR, Rao V. Hybrid cluster based routing protocol for free-space optical mobile ad hoc networks (FSO/RF MANET), Springer Berlin Heidelberg, Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA). 2013; 199:613–20.
8. Jisha G, Samuel P, Paul V. Role of Gateways in MANET Integration Scenarios. Indian Journal of Science and Technology. 2016 Jan; 9(3):1–19
9. Wang J, Lu K. On the mobile relay placement in hybrid MANETs with secure network coding. Security and Communication Networks. 2014; 7(4):738–49.
10. Morreale P, Goncalves A, Silva C. Mobile ad hoc network communication for disaster recovery. International Journal of Space-based and Situated Computing. 2015; 5(3):178–86.
11. Cheng BN, Yuksel M, Kalyanaraman S. Orthogonal rendezvous routing protocol for wireless mesh networks. IEEE/ACM Transactions on Networking (ToN). 2009; 17(2):542–55.
12. Jason R, Madsen M, Daniel J, Tebben T, Dwivedi A, Harshavardhana P, Turner W. Cross layer optimization in assured connectivity tactical mesh networks. IEEE, In Military Communications Conference, USA. 2008; 1–5.
13. Rangarajan J, Baskaran K. Evaluating the Impact of Weather Condition on MANET Routing Protocols. International Journal on Electrical Engineering and Informatics. 2015; 7(3):454.
14. Yang H, Luo H, Ye F, Lu S, Zhang L. Security in mobile ad hoc networks: challenges and solutions. IEEE Wireless Communications. 2004; 11(1):38–47.
15. Wei Z, Tang H, Yu FR, Wang M, Mason P. Security enhancements for mobile ad hoc networks with trust management using uncertain reasoning. IEEE Transactions on, Vehicular Technology. 2014; 63(9):4647–58.
16. Chang JM, Tsou PC, Woungang I, Chao HC, Lai CF. Defending against collaborative attacks by malicious nodes in MANETs, A cooperative bait detection approach. IEEE Systems Journal. 2015; 9(1):65–75.
17. Goncalves A, Silva C, Morreale P. Design of a Mobile Ad Hoc Network Communication App for Disaster Recovery, IEEE. 28th International Conference on Advanced Information Networking and Applications Workshops (WAINA), USA. 2014.
18. Vijayakumar A, Selvamani K. Reputed Packet Delivery Using Efficient Audit Misbehaviour Detection and Monitoring Method in Mobile Ad Hoc Networks. Procedia Computer Science. 2015; 48(1):489–96.
19. Sevincer A, Bhattarai A, Bilgi M, Yuksel M, Pala N. LIGHTNETs: Smart LIGHTing and mobile optical wireless NETworks—A survey. IEEE Communications Surveys and Tutorials. 2013; 15(4):1620–41.
20. Li X, Liu T, Liu Y, Tang Y. Optimized multicast routing algorithm based on tree structure in MANETs. IEEE, Communications, China. 2014; 11(2):90–9.
21. Shang T, Jia J, Wang X. Analysis and design of a multi-transceiver optical cylinder antenna for mobile free space optical communication. Elsevier, Optics and Laser Technology. 2012; 44(8):2384–92.

22. Sanchez- Iborra R, Cano MD, Garcia-Haro J. Performance evaluation of BATMAN routing protocol for VoIP services: a QoE perspective. IEEE Transactions on Wireless Communications. 2014; 13(9):4947–58.
23. Sumathi K, Kumar KS, Sathiyapriya T, Gowri DK. An Investigation on the Impact of Weather Modelling on Various MANET Routing Protocols. Indian Journal of Science and Technology. 2015 Jul; 8(15):1–6.
24. Suresh HN, Varaprasad, Jayanthi G. Notice of Violation of IEEE Publication Principles Designing Energy Routing Protocol With Power Consumption Optimization in MANET. IEEE Transactions on Emerging Topics in Computing. 2014; 2(2):192–7.
25. Paramasivan B, Prakash MJV, Kaliappan M. Development of a secure routing protocol using game theory model in mobile ad hoc networks. IEEE Journal of Communications and Networks. 2015; 17(1):75–83.
26. Qin Y, Huang D, Li B. STARS: a statistical traffic pattern discovery system for MANETs, IEEE, Dependable and Secure Computing. 2014; 11(2):181–92.
27. Zhang R, Sun J, Zhang Y, Huang X. Jamming-resilient secure neighbor discovery in mobile ad hoc networks, IEEE Transactions on 14, Wireless Communications. 2015; 14(10):5588–601.
28. Bezdek JC, Ehrlich R, Full W. FCM: The fuzzy c-means clustering algorithm. Computers and Geosciences. 1984; 10(2):191–203.
29. James JQ, Li VO. A social spider algorithm for global optimization. Applied Soft Computing. 2015; 30:614–27.
30. Koblitz N, Menezes A, Vanstone S. The state of elliptic curve cryptography, Springer US, towards a quarter-century of public key cryptography. 2000. p. 103–23.
31. Zamani E, Soltanaghaei M. The improved overhearing backup AODV protocol in MANET, ACM. Journal of Computer Networks and Communications. New York. 2016; 2016:1–5.
32. Usha S, Radha S. Detection and Avoidance of Node Misbehavior in MANET Based on CLAODV. Indian Journal of Science and Technology. 2011 Oct; 4(10):1–7.