DOI: http://dx.doi.org/10.26483/ijarcs.v9i2.5779

ISSN No. 0976-5697

Volume 9, No. 2, March-April 2018

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

KEY OPTIMIZATION TECHNIQUE IN MOBILE AD HOC NETWORKS

G.Shanthi
Research Scholar
Bharathiyar University
Coimbatore, Tamilnadu, India

M. Ganaga Durga
Assistant Professor
Department of Computer Science
Government Arts College for Women
Sivaganga, Tamilnadu, India

Abstract: In MANET, meta-heuristic algorithm is the major role for selecting optimal route path and security. During optimal routing process the OLSR protocol is modified by using the Fruit Fly Optimization. The FFO algorithm is utilized to locate the ideal and best way to route. After choosing the optimal path Diffie-Hellman(DH) cryptography is used for secure data transmission in Mobile Ad hoc Networks. We have proposed an enhanced DH Cryptographic algorithm based on Particle Swarm Optimization (PSO) Technique for improving the performance of encryption and decryption process and we have shown that Qos of proposed work is better than existing works.

Keywords: Particle Swarm Optimization, Diffie-Hellman Cryptography, Scalar Multiplication, Fruit Fly Optimization(FFO).

I. INTRODUCTION

A Mobile Ad-hoc Network (MANET) is an arrangement of remote versatile hubs that can uninhibitedly and progressively self-compose in subjective and brief system topologies without the need of a wired spine or a concentrated organization. They can be made and utilized whenever, anyplace. In portable Ad-hoc organizes the versatile terminals don't generally have guide radio connects to all the radio terminals in the system, bringing about a circulated multihop arrange, hubs additionally go about as switches and progressively set up interchanges among themselves to frame a framework less remote system.

In bigger and denser system, the Optimized Link State Routing Protocol (OLSR) is created for portable impromptu systems. Every hub chooses an arrangement of its neighbour hubs as "multipoint relays" (MPR). In OLSR, just hubs, chose all things considered MPRs are in charge of sending control movement, proposed for dispersion into the whole system. MPRs give an effective instrument to flooding control movement by diminishing the quantity of transmissions required. Hubs, chose as MPRs, additionally have an exceptional obligation while pronouncing join state data in the system. Without a doubt, the main necessity for OLSR to give most limited way courses to all goals is that MPR hubs pronounce interface state data for their MPR selectors. It is appropriate to expansive and thick portable systems, as the streamlining accomplished utilizing the MPRs functions admirably in this unique circumstance. It works as a table driven, proactive convention, i.e., exchanges topology data with different hubs of the system consistently [1], [2]. OLSR utilizes jump by-bounce routing, i.e., every hub utilizes its nearby data to route packets. OLSR is intended to work in a totally conveyed way and does not rely upon any central entity [3].

A meta-heuristic is an abnormal state issue autonomous algorithmic system that gives an arrangement of rules or techniques to create heuristic enhancement calculations [4]. The word heuristic has its starting point in the old Greek work “heuriskein”, which implies the specialty of finding new systems (rules) to take care of issues. The addition meta, likewise is a Greek word, signifies "upper level philosophy" The term meta-heuristic was presented by F.Glover [5].Particle Swarm Optimization (PSO) calculations are nature-enlivened populace based meta heuristic calculations initially accredited to Eberhart, Kennedy and Shi [6, 7]. The calculations imitate the social conduct of winged animals running and fishes tutoring. Beginning structure a haphazardly disseminated set of particles (potential arrangements), the calculations attempt to enhance the arrangements as indicated by a quality measure (wellness work). The impromptu creation is preformed through moving the particles around the pursuit space by methods for an arrangement of straightforward numerical articulations which demonstrate some between molecule correspondences. These numerical articulations, in their least complex and most essential shape, recommend the development of every particle towards its own best experienced position.

Diffie–Hellman Cryptography (DH) is a cryptographic strategy that permits two gatherings that have no earlier information of each other to mutually set up a common unknown key over interchanges channel. This key would then be able to be utilized to encode resulting correspondences utilizing a symmetric key. In this paper EnhancedDiffie-Hellman Cryptography with PSO is proposed [8].

The rest of the paper is organized as follows Section II provides some related works. Section III provides detailed methodology of proposed work. The simulation results and discussions are presented in section IV. Finally, Section V concludes the paper.

II. RELATED WORKS

Shuaishuai Tan et al. have proposed a trust based routing system, a trust thinking model taking into account fuzzy Petri net [9] is used to evaluate the put stock in estimation of an adaptable hub, and a trust based coordinating figuring is proposed to avoid poisonous or exchanged off hubs however much as could be normal. The exchanged off hubs should in

like manner be kept up a key separation from as they can't give standard organizations any more. Additionally, build up the OLSR tradition by fusing the trust model and trust based directing computation called the FPNT-OLSR tradition.

In a MANET, adroit and flexible aggressors may endeavor to capture, adhere or piece information parcels heading out from source to an objective by SajalSarkar and Raja Datta in 2017 [10]. In proposed beguilement, at each arrange the source hub screens the open different ways, the remaining information exchange capacity of the ways and the method of the aggressors from the information collected in the midst of the past arrange. In see of these discernments, the source hub chooses a way for information communication and trading technique among the different built up ways between the source hub and the goal hub. Execution examination and numerical results illustrate that proposed plot finishes basic execution picks up as distant as remaining transmission capacity utilization, typical end-to-end delay, packet movement extent, routing overhead and security.

In 2017 Mingchuan Zhang et al. [11] have illustrated the bio-inspired cross breed trusted directing convention with respects to trusted assessment, Subterranean insect Colony Optimization (ACO) and Physarum Autonomic Optimization (PAO). At first, this paper brought the cross-layer insight into ACO to get shrewd ants. At that point, it can separate the framework into different zones. Interior each zone, the course table is kept up proactively by the sharp ants which can distinguish concerned parameters. Among zones, the quick ants are sent to responsively find courses to objectives while identifying concerned parameters. Moreover, B-iHTRP utilizes PAO to select the perfect one from the found courses and autonomic accomplice to upgrade the adjacent courses over the span of multi-zone correspondence session.

Decreasing Topology Control (TC) action is a standout among the most basic issues that should to be measured for directing conventions by AbdelaliBoushabet.al. in 2017 [12]. Optimized Interface State Directing (OLSR) is a standout among the most predominant steering conventions for Versatile Advertisement hoc Systems (MANETs), in OLSR each hub spreads TC messages all through the MANET. Solitary hubs utilize this information to handle courses to all objectives. With a particular conclusion objective to decrease TC messages overheads, OLSR utilizes a Multipoint Transfers (MPR) assurance calculation. The proposed methods were utilized to select MPR by utilizing a direct alters in OLSR convention without additional hailing overheads.

In 2017 Stratis Kanarachos et al. [13] have proposed the to begin with run by reflecting this natural product fly behavior and making it as a way to viably address multi-parameter optimization issues. To study its execution an examination was done on ten logical and three truss optimization issues. The results were differentiated with those gotten utilizing twelve best in lesson optimization calculations and assert its incredible and healthy execution. An affectability examination and an appraisal of its execution beneath parallel preparing were driven. The proposed calculation has fair a couple of tuning parameters, is normal, and multi-faceted, empowering application to complex n-dimensional arrange optimization issues.

Cognitive agent based trust model for directing with Identity based cryptography has been proposed by G. Shanthi and M. Ganagadurga [14]. Believe esteem for proficient believe directing has been evaluated utilizing the proposed cognitive agent which is created with the Behaviors-Observations-Beliefs (BOB) show. After the estimation of believe esteem for each cognitive agent, course way has been chosen by selecting the greatest way believe esteem. For securable transmission, Identity based cryptography moreover proposed in this paper. Source sent the information with the ID of the goal and the information was unscrambled when it come to the goal utilizing the ID based cryptography.

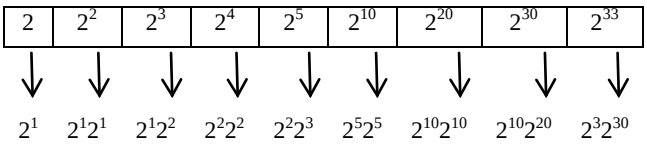
The information communication utilizing Cognitive Radio enabled with MANET has been proposed by G. Shanthi and M. Ganagadurga [15]. Believe esteem for profitable believe directing has been assessed utilizing the proposed cognitive specialist which is made with the Behaviors-Observations-Beliefs (Bob) model. After the estimation of believe esteem for each cognitive agent, course way has been chosen by choosing the most extraordinary way believe regard. The Fruit Fly Optimization calculation is utilized to find the perfect and best way to route. In the wake of selecting the ideal way, Homomorphic Encryption (HE) is utilized for secure information transmission.

III. METHODOLOGY

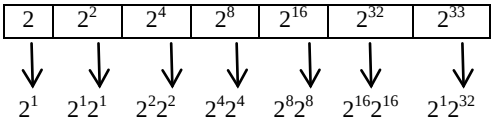
For secure data transmission, enhanced Diffie-Hellman cryptography based on Particle Swarm Optimization is proposed after the establishing the optimal path using FFO [14].

3.1. Problem Statement

In the DH method, the public key of the users is calculated as the total number of scalar multiplication for a given private key value. For example, if we assign the private key value as 33 and primitive root value as 2 for user 1, additional sequence of the public key is generated as follows,



The additional sequence of the above length is 9. So integers of this additional sequence are depicted as, {1, 2, 3, 4, 5, 10, 20, 30, 33} where each integer is calculated as $I_i=I_j+I_k$, where $I_j$and I_k denote the previous two integers (i, j are need not different). Also, we can generate the additional sequence with length 7 for the same the private key value 33. It is shown as below



Different sequence lengths for one key value degrade the performance of the encryption and decryption of the message. The main objective of this proposed approach is to optimize the

additional sequence length of the scalar multiplication i.e. minimizing the length or selecting the minimal length from the various sequence lengths.

3.2. Proposed Work: Enhanced Diffie-Hellman cryptography based on Particle Swarm Optimization.

At first particles or solutions from PSO algorithm are initialized. Then the fitness value of each particle is determined. From the estimated fitness values, pbest (Personal best position) and gbest (Global best position) values are calculated. The particles are updated till get the optimal solution and finally terminated.

a. Encryption

- Additional sequence lengths are initialized as solutions or particles in this approach. Two sets of particles are initialized for both users.

$$\left.\begin{aligned} A1 &= \{X_{11}, X_{12}, \ldots\ldots, X_{1M}\} \text{ for user 1} \\ A2 &= \{X_{21}, X_{22}, \ldots\ldots, X_{2N}\} \text{ for user 2} \end{aligned}\right\} \quad (1)$$

Where, X_{1M} and X_{2N} are represent the Mth and Nth solutions those are defined as follows

$$\left.\begin{aligned} X_{1M} &= \{X_1, X_2, \ldots\ldots..X_m\} \\ X_{2N} &= \{X_1, X_2, \ldots\ldots\ldots X_n\} \end{aligned}\right\} \quad (2)$$

Where, X_m and X_n represent $m^{th}$and n^{th} random prime integers of given private keys R1 and R2.

- Minimum of less particle or sequence length is calculated as fitness value to the solutions. A particle which satisfies this fitness is selected as an optimal solution. The fitness of the particle is considered as P_{best} value. Then, if the fitness of the particle is less than P_{best} value (fit (particle) <Pbest), it is considered as new P_{best}. The best value of neighbors is considered as G_{best} value.
- Until find out the optimal solution, the particles are updated to the new point and above-described process is repeated.
- Above phases are continued until select the minimal sequence length of scalar multiplication. Then the optimized sequence length is used to find out the shared secret key which is also known as an optimized shared secret key (S_{opt}).
- Using the optimized shared secret key (S_{opt}), data or message (M) from the source is encrypted as follows,

$$E = M + Sopt \quad (3)$$

- Then the encrypted message (E) is transmitted to the destination through the optimal path using FFO.

b. Decryption

- At the destination, the encrypted message is decrypted by subtracting that with the same optimized shared secret key. Decryption is calculated as follows,

$$D = E - Sopt \quad (4)$$

$$= M + Sopt – Sopt \quad (5)$$

$$D = M \quad (6)$$

IV. SIMULATION

Our proposed work is simulated using the Network Simulator (NS2). In the simulation, mobile nodes in MANET will perform with in the region 1000m×1000m with the simulation time 50secs. All nodes have the same transmission range of 250 meters. All nodes have the same transmission range of 250 meters. Each node in the region has 0.660W transmitting power and has 0.395W receiving power. Table 1 shows the simulation parameters of our work.

Table I. Simulation Parameters

Parameter	*Value*
No of nodes	*150*
Area	*1000×1000*
Mac	*802.11*
Simulation time	*50s*
Transmission range	*250m*
Packet size	*500*
Transmitting power	*0.660W*
Receiving power	*0.395W*
Rate	*50 kbps*

4.1. Performance based on nodes

In this Section, performance metrics such as energy consumption, delay, throughput, delivery ratio, packet drop are analyzed by varying nodes. Our proposed work DH-PSO is compared with the existing works CATR [14] and OLSR-FFO [15].

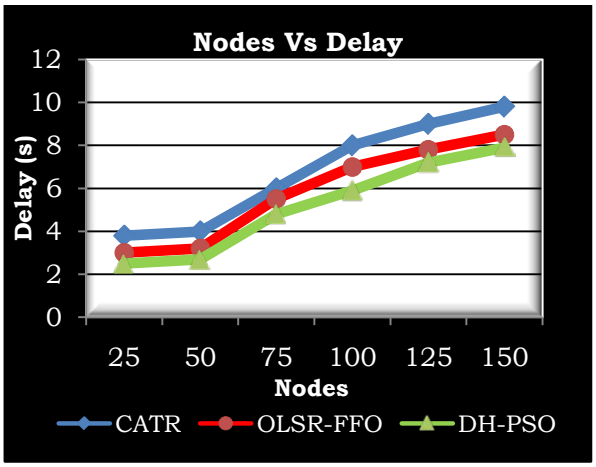


Figure 1: Nodes Vs Delay

Figure 1 shows the Delay time of the proposed work DH-PSO with the existing works CATR and OLSR-FFO Compared to the existing works, Delay time of our proposed work is reduced. When the number of nodes increases, Delay time also decreases.

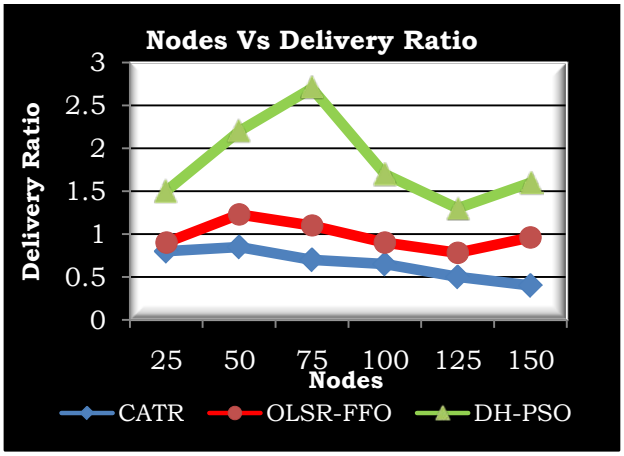


Figure 2: Nodes Vs Delivery ratio

Figure 2 shows the Delivery ratio of the proposed work DH-PSO with the existing works CATR and OLSR-FFO Compared to the existing works; Delivery ratio of our proposed work is improved. When the number of nodes increases, Delivery ratio also increases.

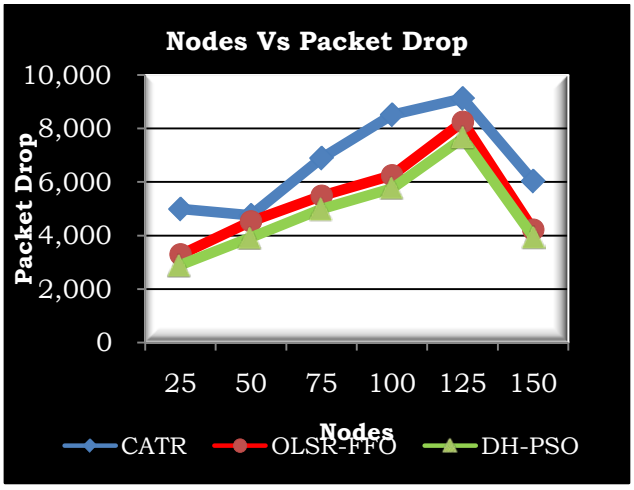


Figure 3: Nodes Vs Packet drop

Figure 3 shows the packet drop of the proposed work DH-PSO with the existing works CATR and OLSR-FFO Compared to the existing works packet drop of our proposed work is reduced. When the number of nodes increases, packet drop also decreases.

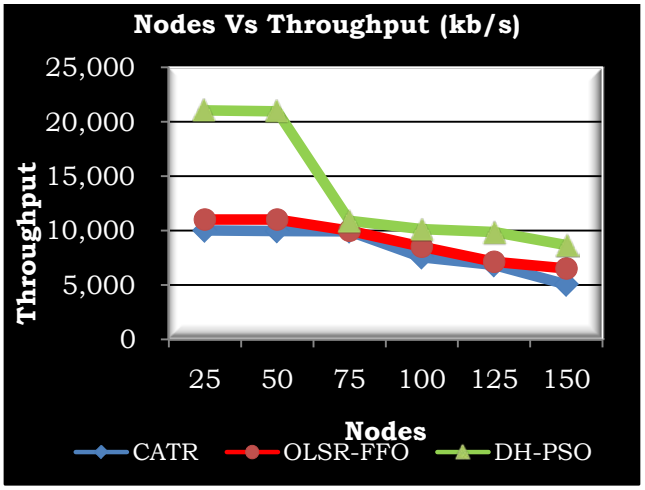


Figure 4: Nodes Vs Throughput

Figure 4 shows the throughput of the proposed work DH-PSO with the existing works CATR and OLSR-FFO Compared to the existing works; Throughput of our proposed work is improved. When the number of nodes increases, throughput also increases.

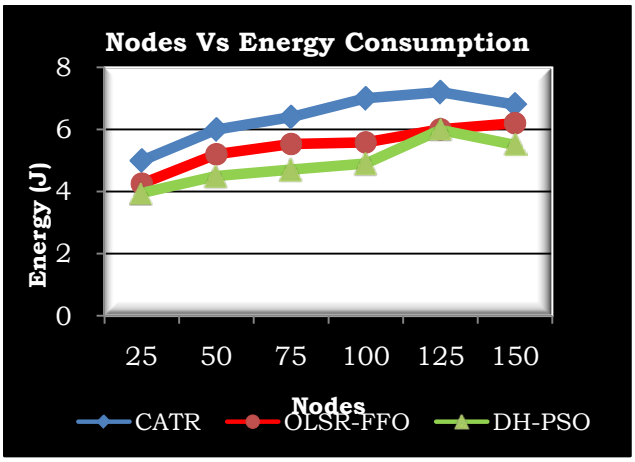


Figure 5: Nodes Vs Energy consumption

Figure 5 shows the Energy consumption of the proposed work DH-PSO with the existing works CATR and OLSR-FFO Compared to the existing works; Energy consumption of our proposed work is improved. When the number of nodes increases Energy consumption also decreases.

4.2. Performance based on speed

In this section, performance metrics such as energy consumption, delay, throughput, delivery ratio, packet drop are evaluated by varying speed. Our proposed work DH-PSO is compared with the existing works CATR [14] and OLSR-FFO [15].

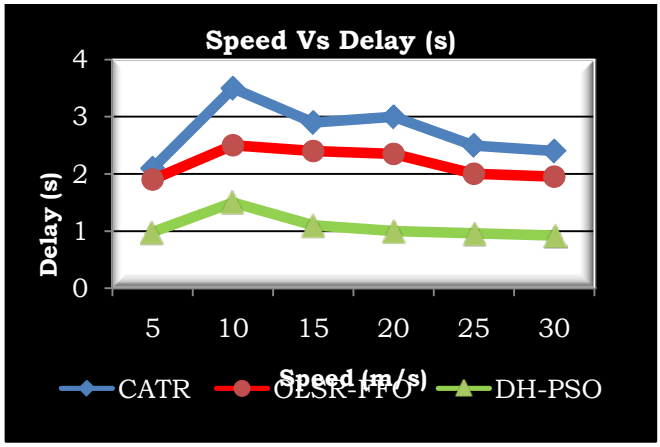


Figure 6: Speed Vs Delay

Figure 6 shows the Delay time of the proposed work DH-PSO with the existing works CATR and OLSR-FFO Compared to the existing works, Delay time of our proposed work is reduced. When the speed increases, Delay time also decreases.

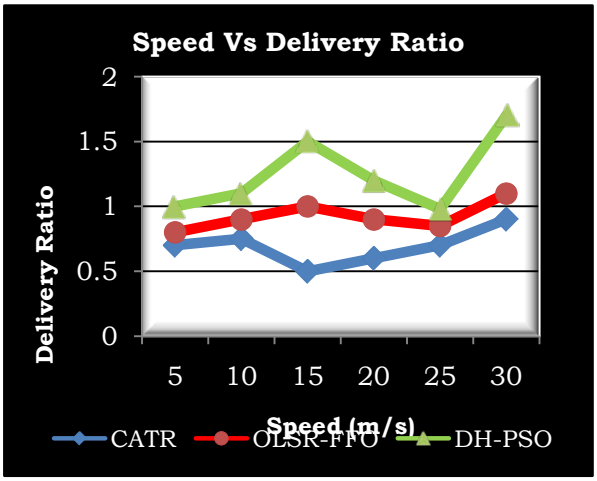


Figure 7: Speed Vs Delivery ratio

Figure 7 shows the Delivery ratio of the proposed work DH-PSO with the existing works CATR and OLSR-FFO Compared to the existing works; Delivery ratio of our proposed work is improved. When the Speed increases, Delivery ratio also increases.

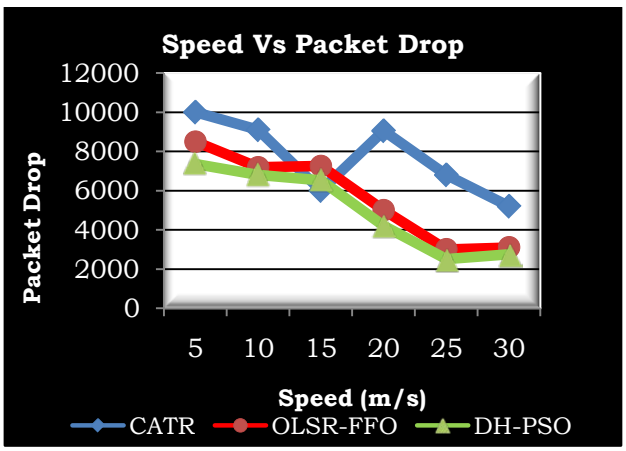


Figure 8: Speed Vs Packet drop

Figure 8 shows the packet drop of the proposed work DH-PSO with the existing works CATR and OLSR-FFO Compared to the existing works packet drop of our proposed work is reduced. When the Speed increases, packet drop also decreases.

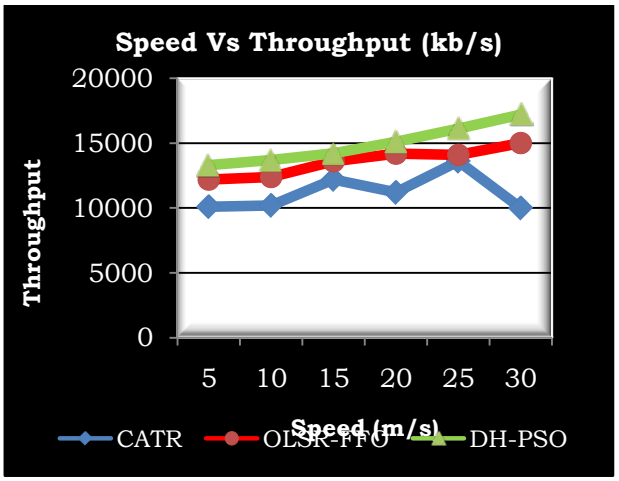


Figure 9: Speed Vs Throughput

Figure 9 shows the throughput of the proposed work DH-PSO with the existing works CATR and OLSR-FFO Compared to the existing works; Throughput of our proposed work is improved. When the Speed increases, throughput also increases.

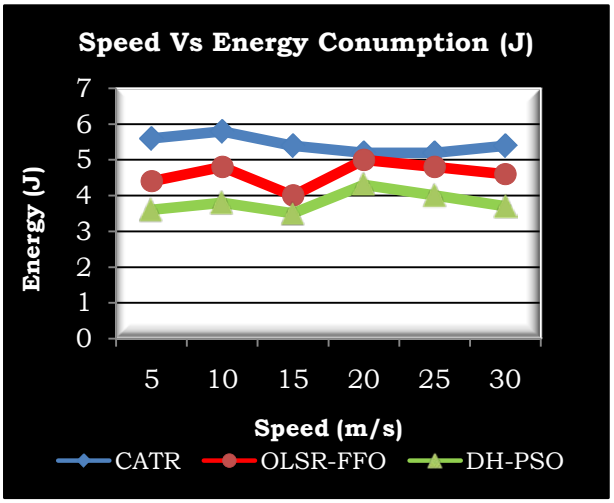


Figure 10: Speed Vs Energy consumption

Figure 10 shows the Energy consumption of the proposed work DH-PSO with the existing works CATR and OLSR-FFO Compared to the existing works; Energy consumption of our proposed work is improved. When the Speed increases Energy consumption also decreases.

V. CONCLUSION

Optimal route path is identified using Fruit Fly Optimization (FFO) and has been simulated using the network simulator NS2. After getting optimal solution using FFO for securable transmission Enhanced Diffie-Hellman Cryptography based on Particle Swarm Optimization technique in Mobile Ad-hoc Network has been proposed. Our proposed work minimizes the additional sequence length of scalar multiplication.

Minimal sequence length raises the speed of encryption and decryption process. Normally when encryption and decryption process is done at fast, no one can attack on packet to reveal the secret, so confidentiality is achieving. Network load is reduced since their key exchange mechanism is simple. Our proposed work achieved these objectives. From the simulation results, we have shown that our work has better QoS compared to the existing works CATR and OLSR-FFO and also energy consumption of our proposed work has been improved with existing works.

REFERENCES

[1] P. Jacquet, P. Minet, P. Muhlethaler, N. Rivierre. Increasing reliability in cable free radio LANs: Low level forwarding in HIPERLAN. Wireless Personal Communications, 1996.

[2] Qayyum, L. Viennot, A. Laouiti. Multipoint relaying: An efficient technique for flooding in mobile wireless networks. 35th Annual Hawaii International Conference on System Sciences (HICSS'2001).

[3] www.ietf.org/rfc/rfc3626.

[4] Kaveh, "Particle Swarm Optimization", Advances in Metaheuristic Algorithms for Optimal Design of Structures, pp. 11-43, 2016.

[5] Glover F, Kochenberger GA (eds) (2003) Handbook of metaheuristics. Kluwer Academic Publishers, Dordrecht

[6] Kennedy J, Eberhart R (1995) Particle swarm optimization. In: Proceedings of IEEE international conference on neural networks, vol 4, pp 1942–1948

[7] Shi Y, Eberhart R (1998) A modified particle swarm optimizer. In: Proceedings of IEEE World congress on computational intelligence. In: The 1998 I.E. international conference on evolutionary computation

[8] Eesti Infotehnoloogia Kolledz Diffie-Hellman key exchange Essay Sandra Netsajeva Tallinn 2009.

[9] Tan, S., Li, X. and Dong, Q. (2015) 'Trust based routing mechanism for securing OSLR-based MANET', Ad Hoc Networks, vol. 30, pp. 84-98.

[10] Sarkar, S. and Datta, R., 2016. A game theoretic framework for stochastic multipath routing in self-organized MANETs. Pervasive and Mobile Computing.pp.1-18

[11] Zhang, M., Yang, M., Wu, Q., Zheng, R. and Zhu, J., 2017. Smart perception and autonomic optimization: A novel bio-inspired hybrid routing protocol for MANETs. Future Generation Computer Systems,pp.1-18.

[12] Boushaba, A., Benabbou, A., Benabbou, R., Zahi, A. and Oumsis, M., 2015. Multi-point relay selection strategies to reduce topology control traffic for OLSR protocol in MANETs. Journal of Network and Computer Applications, Vol.53, pp.91-102.

[13] Kanarachos, S., Griffin, J. and Fitzpatrick, M.E., 2017. Efficient trust optimization using the contrast-based fruit fly optimization algorithm. Computers & Structures, Vol.182, pp.137-148.

[14] Govindan Shanthi, Meenakshi Sundaram Ganaga Durga Cognitive-based routing model with identity-based cryptography in MANET Int. J. Mobile Network Design and Innovation, Vol. X, No. Y, 200x (forthcoming inderscience publications)

[15] G. Shanthi, M. Ganaga Durga Secure and Trusted Optimal Routing Model Using Fruit Fly Optimization for Cognitive Radio Based MANET, International Journal of Pure and Applied Mathematics Volume 118 No. 7 2018, 605-614 ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)