Secure and Efficient Data Transmission using AODVACO-PSO-DHKE Methodology in ad-hoc Network

Arudra Annepu[1], Madalai Jayaprasad[2]

[1,2]*Rajiv Gandhi Institute of Technology, India*
(E-mail: yarudra@gmail.com)

Abstract—Mobile Ad-hoc Network (MANETs) has numerous Sensor nodes, which is deployed within the region it is used for transmitting the infor-mation depends on the location of Sensor Nodes. The nodes are free to move randomly. The efficient route establishment using ad-hoc on demand distance vector (AODV) routing protocol, which is optimized using Ant Colony Optimization (ACO) techniques. The Particle Swarm Optimization (PSO) techniques is used for clustering/grouping of sensor nodes in the networks. Each packets are secured using Diffie-Hellman key exchange (DHKE) techniques in sensor networks. The AODV Routing protocol is used for transmitting the data packets from one node to another and for choosing the shortest path, the optimization used is ACO. The DHKE methodology provides Secret key in both users. Hence, AODVACO-PSO-DHKE techniques is used for providing secured and effective transmission of data by improving parameters such as throughput, routing overhead, delay and energy consumption in secured environment. Therefore, Throughput increases (10%) with decrease in routing overhead (7%), delay (8%), energy consumption (5%) in AODVACO-PSO-DHKE than AODV-PSO Methodology.

Keywords—*Ad-hoc On Demand Distance Vector; Ant Colony Optimization; Diffie-Hellman key exchange; Particle Swarm Optimization; Wireless Sensor Network.*

I. INTRODUCTION

WSN is an on growing research topic in the field of communication system. Usually, it consists of a number of sensor nodes which are interconnected through wireless links to monitor physical or environmental conditions, like sound, temperature, and motion [1]. The less cost makes this possible to have a network of thousands of sensors, thereby enhance the reliability and accuracy of data and the area coverage [2]. But the drawbacks of the WSN are that it has limited battery power, limited storage and computation capabilities, prone to the security attacks and have limited bandwidth to communicate [3]. Clustering in WSN is performed to minimize the energy consumption and also to reduce the data transmission over the network that is required to transmit the message to the BS. The CH becomes responsible for communication, which results into prolonged network lifetime [4]. A CH aggregates the data collected by the leaf node in its cluster, and sends the aggregation to the base-station. The Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol is used to improve network-lifetime in the networks [5]. The IDS nodes must be set in sniff mode to perform ABM (Anti-Blackhole Mechanism) function. The IDS nodes are deployed in MANETs to detect and prevent selective Blackhole Mechanism [6].

The IDS nodes must be set in sniff mode to perform ABM (Anti-Blackhole Mechanism) function. The IDS nodes are deployed in MANETs to detect and prevent selective Blackhole Mechanism [7]. A secure hierarchical S-LEACH protocol is introduced to provide high security in the LEACH protocol. In this way, S-LEACH improves the energy-efficiency and extend the lifetime of the network [8]. Secure solution for LEACH has been introduced for forming clustering dynamically and periodically, which is known as RLEACH techniques. The major problem in RLEACH is orphan node because of random pair-wish key. So, to overcome this orphan node problem, the efficient cryptography method is introduced [9]. RLEACH resists too many attacks like spoofed, alter and re-played information, sinkhole, wormhole, selective forwarding, HELLO flooding and Sybil attack. A new secure routing protocol with ID-based signature method for cluster-based WSNs is dependent on the hardness [10]. The Ad hoc On-Demand Distance Routing Protocol-Ant Colony Optimization algorithm is used for routing optimization. Particle swarm optimization (PSO) algorithm is used for clustering and Diffie–Hellman Key exchange algorithm is introduced for security. The AODVACO-PSO-DHKE system provides better results in throughput (10%), routing overhead (7%), delay (8%) and energy consumption (5%) compared to the existing AODV-PSO [16] Methodology.

The rest of this paper is organized as follows: Section 2, reports on related work. Section 3, presents a review on "AODVACO-PSO-DHKE" Methodology in ad-hoc network. Section 4, demonstrated the simulation parameters of the "AODVACO-PSO-DHKE" and Section 5 indicates the conclusion of this research work.

II. RELATED WORK

L. Bhasker [11] has introduced a genetically derived secure cluster-based data aggregation in WSN. The cluster-heads are designated based on the node connectivity, which acts as a data aggregator. A data aggregator technique offers authenticity, confidentiality and integrity. In that initially the cluster heads are selected based on the node connectivity, which acts as a data aggregator. The delivery ratio of packet send can be determined in the future.

U. Vasala, and G. R. Sakthidharan [12] presented the Effective Key Management in Dynamic WS Networks system to provide secure communication in dynamic WSNs, which is characterized by node mobility. The CL-EKM supports economic key updates once a node leaves or joins a cluster and ensures forward and backward key secrecy. This system does not provide more security.

Thomas R. Halford *et al* [13] has proposed Energy-efficient Group Key Agreement protocol for WSNs, achieves best possible approximation in polynomial time. The Lightweight PKAs should be augmented and addressed further with energy-efficient mechanisms for effective group key agreement of datas. To characterize the minimum number of public transmissions a desired integer number of statistically independent secret keys.

K. Shanmugam *et al* [14] has proposed effective clustering to enhance the system performance of WSNs using SET-IBS and SET-DTA protocols. Secure and efficient data transmission using SET protocol showed the falsified sub-aggregate attack by a few compromised nodes. SET Protocol have better performance than the existing CWSNs secure protocols, in-case of energy consumption and overhead.

M. Elhoseny *et al.* [15] introduced a novel encryption schema based on Elliptic Curve Cryptography (ECC) and Homomorphic Encryption to secure data transmission in WSN. This system prevents passive attack, CH compromised attack, and brute force attack. Hence, hybrid method is used further for enhancing the secure data transmission in the networks with different kinds of attacks.

III. AODVACO-PSO-DHKE SYSTEM

The security is the major concern in any kind of wireless ad-hoc networks. In this paper, AODVACO-PSO-DHKE method is introduced which will provide the very high secured communication in sensor network. Also the AODVACO-PSO-DHKE system will secure the information from the various attacks. Hence, DHKE provides less computational time with less storage. DHKE shares different shares different private and public key exponents. Hence, DHKE diminishes the memory requirements for storing both public and private key with two different secret keys. The two different DHKE Occurrences such as T1=r1s1 and T2=r2s2. The public key (e) and private key (d) should gratify the following equations ed≡1 mod Ø (T1) and ed≡1 mod Ø (T2). Routing for MANET is a Dynamic Optimization Problem as the search space changes with the time. The routing policy has defined the rule, which specifies what node has to communicate with next node, which is on the way to reach the destination node.

This system consists of eight major steps: 1) Mobile node development, 2) Clustering using PSO, 3) cluster head selection based on node weight, 4) router estimation using AODVACO, 5) data received to cluster head, 6) Encryption by DHKE, 7) Successfully receiving the data, 8) decryption process. The Overall block diagram of the AODVACO-PSO-DHKE system is shown in the below Figure.1.

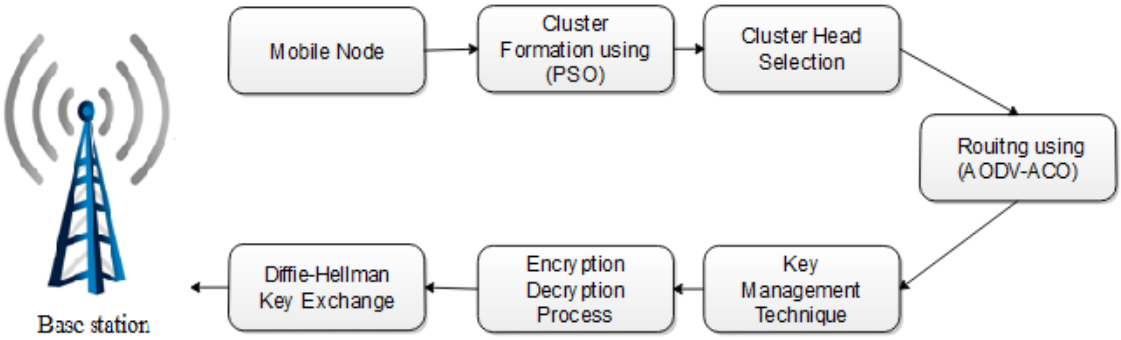

Fig. 1. Block Diagram of PSO-AODVACO-DHKE system

A. Clustering based Particle Swarm Optimization Algorithm

The PSO based clustering algorithm has 3 steps: Particle initialization, fitness function calculation and position update. PSO is an emphasis based optimal algorithm and that PSO technique is introduced with a populace of dynamic solutions for finding ideal route by updating generations. In the search process, PSO combines local fitness with global fitness. The particle alters are used to predict the present position of the authentic data as well as relying on the related data of neighboring particles, which finds the optimal solution with the number of iterations.

The particle is updated in each iteration by two best esteems, for example, initial one is the best fitness. The Best fitness Pbst is achieved by the individual particle. Another best value is obtained from the set of P_{bst} values globally and it is represented by g_{bst}. Particle initialization: In an initial step, particles are deployed randomly and K means clustering algorithm are applied to get centroids for making clusters. These centroids are optimized by PSO algorithm. Clustering scatter presented by the particles are evaluated in a fitness functions. The fitness functions take the generated cluster scatter as an input parameters and return a numerical result to validate the correctness of the clustering scatter. The validation formula is used as a fitness function in equation 1. "m" denotes total numbers of element in the dataset, $D_j^{C_j}$: element belongs to j^{th} cluster, O_j: Origin of j^{th} cluster

$$F = \frac{1}{m}\sum_{i=1}^{m}\left\| o_j, D_j^{C_j} \right\| \quad (1)$$

In PSO are used for obtaining the best particle for cluster head. This can be obtained by finding the distance between the optimized centroid with all the neighborhood nodes. The d best is calculated and the cluster is selected to correspond to the minimum d_best. The local best and global best is explained in the equation 2 and 3. This will be repeated for some set of particles 20xNp, from this d_best value is generated. Corresponding to this d_best obtain the location of the particle. The above process is repeated again with some iterations to obtain the d_gbst and the corresponding position of the particle is updated. The fitness function is the separation between the centroid of the cluster and neighborhood particles. d_best is as much as least. The position of particle is influenced by velocity. Let $xi(t)$ denotes the particle position i in the search space at time step t.

$$xi(t+1) = xi(t) + vi(t+1) \quad (2)$$

$$vi(t) = vi(t-1) + c1r1(localbest(t) - xi(t-1)) + c2r2(globalbest(t) - xi(t-1)) \quad (3)$$

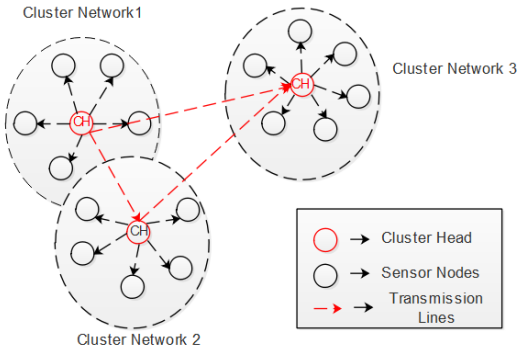

Fig. 2. Basic Clustering in Mobile ad-hoc network

In Figure.2 the Sensor Nodes are grouped to-gather to form different cluster networks. The CH is elected for each cluster networks based on the minimum value of degree. The job of the cluster-head is to assemble information from their neighboring nodes and pass it on to another CH in different Networks. The CHs broadcast a confirmation message that includes a time slot schedule to be used by their cluster members for communication during the steady-state phase. In "AODVACO-PSO-DHKE" methodology, the clusters are changed with the different rounds in the networks, which is known as dynamic clustering.

B. AODV-Routing Protocol

The routing protocol is intended for use by mobile nodes in ad hoc network. The AODV is designed to decrease the dissemination of overhead and control traffic. The AODV routing protocol deals with two functions such as Route Discovery and Route Maintenance. The finding of the fresh route is decided by Route Discovery function and the discovery of link breaks and repair of an existing route is decided by Route Maintenance function. The reactive protocol does not maintain permanent route table. AODV is quickly able to analyse the changes in network topology. The Data transfer of AODV routing Protocols are given in Figure.3

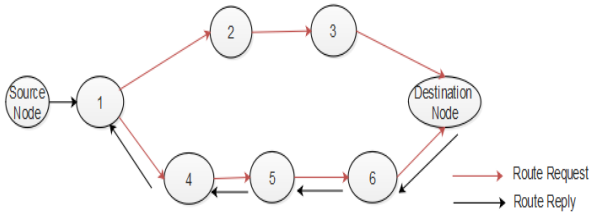

Fig. 3: AODV Routing Protocols-Data Transfer

Route optimization using ACO algorithm

ACO routing algorithm take attraction from the characteristics of ants in nature and from the related field of ACO to resolve the problems of routing in sensor networks. The main source of motivation is found in the capacity of certain kinds of ants to search the shortest path among their nest and a food sources using Pheromone (Impulsive Chemical Substance). Ant leave traces of pheromone as they migrate

between sources to destination. Ants specially go in the course of high pheromone intensities in search of food. The higher levels of pheromone are received, when minimum paths are finished faster. The positive strengthening process allows the colony as a whole to touch on the shortest path.

The probability for ant l at node k moving to node l at generation u is defined as in equation 4.

$$Q^{K}_{J,L}(u) = \frac{tj,k(u)d^{-\beta}_{j,k}}{\sum_{u\varepsilon}\Gamma^{kt}\, j, v^{d}_{j,v}{}^{-\beta}}, k \in \Gamma^{k}_{j} \qquad (4)$$

Where is the intensity of the pheromone on edge is the distance between nodes i and k, is the set of nodes that endure to be visited by ant k position at node I to make the solution feasible and

Once all the ants have built their tours, the pheromone is updated on all edges according to a global pheromone-updating rule in equation 5, 6 and 7.

$$t_{j,k}(t+1) = (1-\rho)_{j,k}(t) + \Delta t_{j,k}(t) \qquad (5)$$

Where

$$\Delta t_{j,k}(t) = \sum_{K=1}^{NP} \Delta t^{k}_{j,k}(t) \qquad (6)$$

$$\Delta t_{j,k}(t) = \left\{ \begin{array}{l} \frac{Q}{LK}, if\,(j,k) \in tourdonebyantk \\ 0, otherwise \end{array} \right\} \qquad (7)$$

It is the pheromone decay parameter where it represents the trail evaporation when the ant chosen a city and decide to move L_k is the length of the tour accomplished by ant k and m is the no. of ants [17].

C. Key Management Technique

After cluster head selection, key management method is applied. In key management method, each cluster head recollects the public key of its member nodes only and turn as a router when dealing with nodes of other cluster members. With the help of this method, the overhead on centralized key management systems is abridged. Furthermore, the need of each node for storing all public keys is reduced thus diminishing the storage overhead on each node.

After providing keys to the cluster head it is indispensable for encrypting the information in the nodes hence some encryption approaches are used to prevent the information from attacks. The comprehensive clarification of encryption is as follows.

1) Encryption

Encryption is the procedure of converting data or information into a code, particularly to prevent unauthorized access. The encryption of information can be performed by Diffie–Hellman Key Exchange (DHKE) algorithm. The comprehensive explanation of this algorithm is as follows.

2) Diffie-Hellman Key Exchange Algorithm

Diffie-Hellman key exchange is a precise technique of exchanging cryptographic keys. It is one among the earliest practical examples of key exchange functional within the field of cryptography. The DHKE technique permits two parties that have no prior knowledge of each other to jointly start a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications with the help of a symmetric key cipher. Though Diffie-Hellman key agreement itself is an anonymous (non-authenticated) key-agreement protocol, it gives the basis for a variety of authenticated protocols and is utilized to give perfect forward secrecy in Transport Layer Security's ephemeral modes (mentioned to as (Elliptic-Curve Diffie Hellman) EDH or (Diffie Hellman key exchange) DHE contingent on the cipher suite). Figure.4 illustrates Diffie Hellman Key Exchange Method block diagram.

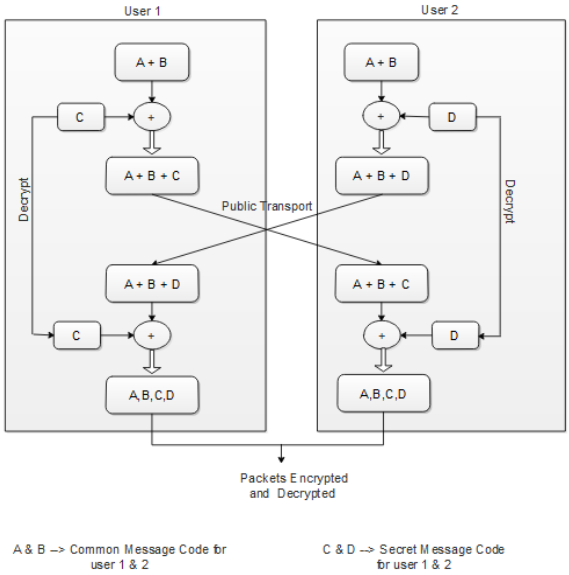

Fig. 4. Diffie–Hellman Key Exchange Method

The DHKE Cryptography is the popular cryptography system, which is used for security purpose in the wide range of networks. The security border should be elevated in the DHKE. The most difficult part of DHKE cryptography is public and private key generation. The prime numbers p and q are created by employing the DHKE cryptography. C and D are Secret key for user 1 and 2. The modulus 'n' is subtracted by duplicating P and Q. Both the general population such as private and public keys between the operators exploits the number. The one user at the end, sends plain text to the encrypted public key with secret key.

Key Generation		
Select	p, q	
p,q both are prime	$p \neq q$	
Calculate	$n = pxq$	
Calculate	$\varphi(n) = (p-1)x(q-1)$	
Select integer	e	$\gcd(\varphi(n), e) = 1; 1 < e < \varphi(n)$
Calculate	d	

Public key	$KU = \{e, n\}$		
Private key	$KR = \{d, n\}$		
Secret Key	C and D		
Encryption		Decryption	
Plain text	$M < n$	Cipher text	C
Cipher text	$C = M^e \pmod n$	Plain text	$M = C^d \pmod n$

The Figure.5. Shows the flow chart of the overall routing process. Here a finite number of mobile nodes is organized in the specified area and initially, source and destination are assigned. Once source and destination are defined then source node broadcast an RREQ to all the neighbor nodes. The route establishment method is done using AODV routing protocol. The AODV routing protocol is optimized using ACO technique for efficient results. The grouping of sensor node is optimized using PSO optimization techniques. The secured transmission using DHKE cryptography is used. The overall flow chart is illustrated below in Figure.5.

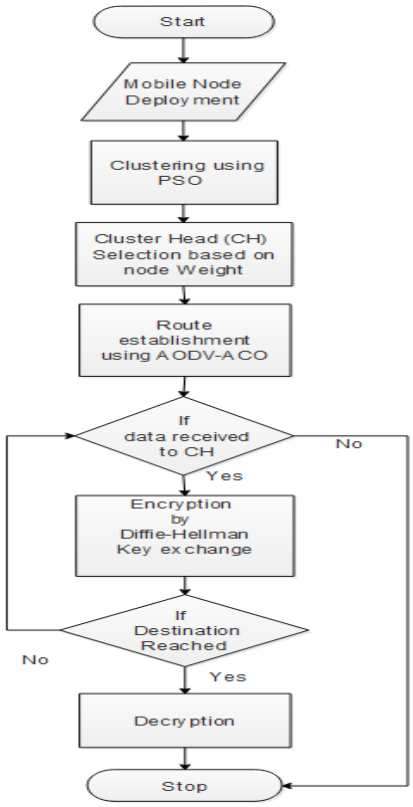

Fig. 5. Flow chart of Overall AODV-ACO-PSO-DHKE Method

IV. RESULT AND DISCUSSION

The AODV-ACO-PSO-DHKE method is implemented in NS2 to achieve efficient clustering and routing for transmission of data using AODV routing protocol with ACO optimization algorithm. The complete work is done by using the I7 system with 8 GB RAM. The PSO algorithm is used to obtain the optimized path and DHKE for secure transmission through the wireless mobile nodes.

This section gives a detailed view of the results that are obtained using AODV-ACO and DHKE algorithm. AODV-ACO-PSO-DHKE algorithm is used for providing security to the messages contained in the nodes. The experimental results and the performance of Throughput, routing overhead, delay and energy are compared with the existing method. The performance is calculated by measuring the throughput, routing overhead, delay and energy consumption parameters. Throughput, Packet delivery ratio is increased with a decrease in routing overhead. The Performance metrics is given below;

Throughput: Throughput is calculated based on total packets received at the destination node by total network time, which is expressed in equation 8.

$$Throughput = \frac{Total\ packets\ received\ at\ the\ destination\ node}{Total\ simulation\ time} \quad (8)$$

Routing Overhead: Routing Overhead is the quantity of routing packets requires for network communication, which is divided by a total number of delivered data packets, explained in equation 9.

$$Roughting\ Overhead = \frac{Total\ no.of\ routing\ packets}{Total\ no.of\ delivered\ data\ packets} \quad (9)$$

Energy consumption: The huge number of hops is equivalent to the huge amount of received energy consumption. A node drops a particular amount of energy for every packet transmission and received.

Delay: Different between Sending time of packets and receiving time of packets is known as delay.

Comparison analysis of AODV-PSO-AES is evaluated by varying the nodes 20, 40, 60, 80 and 100. The figure 6, 7, 8 and 10. Shows the comparison of the Throughput, Routing Overhead, delay and energy Consumption between existing methods. Table.1 and 2, Shows the Comparison between AODVACO-PSO-DHKE Method and AODV-PSO Method. Throughput increases 10 % in AODVACO-PSO-DHKE than AODV-PSO Methodology [16]. Routing overhead decreases 7 % in AODVACO-PSO-DHKE than AODV-PSO Methodology [16].

TABLE I. COMPARISON BETWEEN AODVACO-PSO-DHKE METHOD AND AODV-PSO METHOD

Number of Mobile Nodes	Throughput (Kbps)		Routing Overhead (%)	
	AODV-PSO [16]	AODVACO-PSO-DHKE	AODV-PSO [16]	AODVACO-PSO-DHKE
20	336	376	8292	7828
40	125	142	6234	5893
60	120	133	8455	8246
80	93	101	9345	9204
100	70	93	7123	6960

In Table.2 the comparison between AODVACO-PSO-DHKE Method and AODV-PSO Methodology is addressed. Delay decreases 8 % in AODVACO-PSO-DHKE than AODV-PSO Methodology. Energy Consumption decreases 5 % in AODVACO-PSO-DHKE than AODV-PSO Methodology [16]. Therefore, the QoS parameters values such as Throughput, routing overhead, delay and energy consumption of AODV-PSO are implemented and theoretically referred in below cited paper [16].

TABLE II. COMPARISON BETWEEN AODVACO-PSO-DHKE METHOD AND AODV-PSO METHOD

Number of Mobile Nodes	Delay (Sec)		Energy Consumption (kilo joules)	
	AODV-PSO [16]	AODVACO-PSO-DHKE	AODV-PSO [16]	AODVACO-PSO-DHKE
20	1.286	0.179	21.2012	21.1919
40	1.652	1.359	21.2017	21.1904
60	1.713	1.867	21.6463	21.5930
80	4.064	3.084	21.7648	21.6940
100	2.578	1.693	21.8083	21.7913

Comparison analysis of AODV-PSO-AES is evaluated by varying the nodes 20, 40, 60, 80 and 100. The figure 6, 7, 8 and 10. Shows the comparison of the Throughput, Routing Overhead, delay and energy Consumption between AODV-PSO existing methods.

The Comparison of Nodes vs. throughput between AODV-ACO-PSO-DHKE and AODV-PSO is plotted in Figure.6. The Throughput value is increased in AODV-ACO-PSO-DHKE method, when compared with the AODV-PSO method with different 20, 40, 60 80 and 100 Nodes.

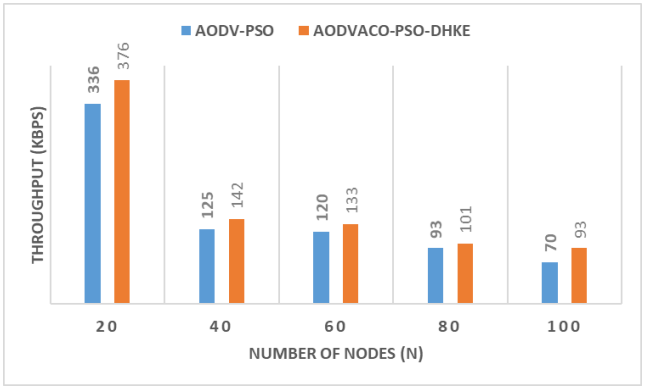

Fig. 6. Node vs. Throughput

The Comparison of Nodes vs. routing overhead between AODV-ACO-PSO-DHKE and AODV-PSO is plotted in Figure.7. The routing overhead is decreased in AODV-ACO-PSO-DHKE method, when compared with the AODV-PSO method by varying different 20, 40, 60 80 and 100 Nodes.

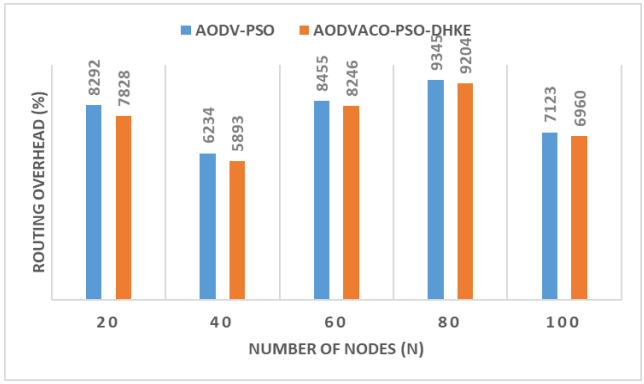

Fig. 7. Node vs. routing overhead

The Comparison of Nodes vs. delay between AODV-ACO-PSO-DHKE and AODV-PSO is plotted in Figure.8. The delay is decreased in AODV-ACO-PSO-DHKE method, when compared with the AODV-PSO method by varying different 20, 40, 60 80 and 100 Nodes.

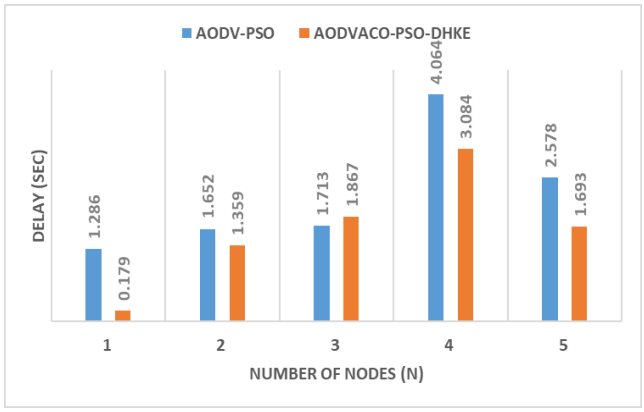

Fig. 8. Node vs. delay

The Comparison of Nodes vs. energy between AODV-ACO-PSO-DHKE and AODV-PSO is plotted in Figure.9. The energy consumption is decreased in AODV-ACO-PSO-DHKE method, when compared with the AODV-PSO method by varying different 20, 40, 60 80 and 100 Nodes.

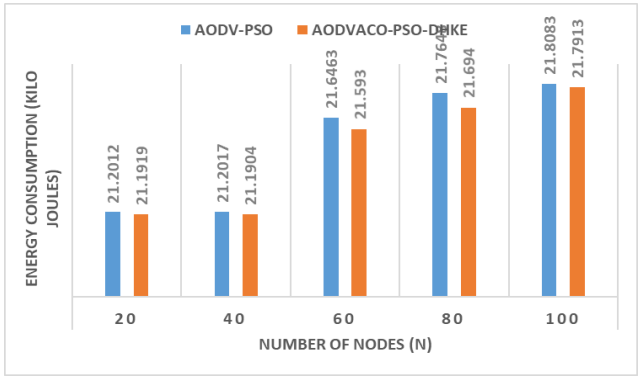

Fig. 9. Node vs. Energy Consumption

Thus, AODVACO-PSO-DHKE techniques effectively used for securing data packets from source to destination in sensor networks with increase in throughput by decreasing routing overhead, delay and energy consumption. Table 3, shows the

simulation parameters of AODVACO-PSO-DHKE Methodology used in NS2. The simulation start time and ending time is 0.0-5.0. The nodes are randomly distributed in the area. The 20, 40, 60, 80 and 100 nodes are distributed randomly. Here, each data packets starts its journey from a random-location to a random destination with randomly chosen speed. In traffic model, the Constant-bit rate (CBR) traffic sources are used with 802_11 MAC Type.

TABLE III. SIMULATION PARAMETERS

Routing algorithm	AODV-ACO
Clustering algorithm	PSO
Security used	DHKE
Simulator used	NS2
Simulation start time	0.000000000
Simulation End time	50.00000000
Random Mobility Model	Random Way point
Propagation Model	Two-ray Ground
Traffic Model	Constant bit Rate (CBR)
Number of mobile nodes	20, 40, 60, 80 and 100
Number of BS Set	One
Antenna Model	Omni Antenna
Minimum speed	28 ms
Network Interface types	Wireless ad-hoc
MAC Type	MAC/802_11
Initial Transmit Power	0.660
Initial Receive Power	0.395
Performance parameters	Throughput, routing overhead, delay and energy consumption

V. CONCLUSION

In "AODVACO-PSO-DHKE" methodology is used for secured data transmission in ad-hoc networks. Hence, for efficient data transmission AODV routing protocol with ACO optimization is used. PSO Clustering takes place for maintaining energy in each nodes. Secure transmission of data from source to destination using DHKE methodology. Thus, overall methodology provide provides better results in term of throughput, routing overhead, delay and energy consumption compared with existing method. Therefore, Throughput increases 10 % in AODVACO-PSO-DHKE than AODV-PSO Methodology, Routing overhead, delay, and Energy consumption decreases 7 %, 8% and 5% in AODVACO-PSO-DHKE than AODV-PSO Methodology. As a Future Scope, hybrid cryptography techniques can be used for improving security and by selecting secured path in case of node failure/false node in the Mobile ad-hoc network.

REFERENCES

[1] Lu, H., Li, J. and Guizani, M., "Secure and efficient data transmission for cluster-based wireless sensor networks," IEEE transactions on parallel and distributed systems, vol. 25, no. 3, pp.750-761, 2014.

[2] Shine, A.V. and Venkadesh, P., "Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks: A Study," International Journal of Engineering and Future Technology™, vol. 5, no. 5, pp.36-42, 2016.

[3] Bhattacharyya, D., Kim, T.H. and Pal, S., "A comparative study of wireless sensor networks and their routing protocols," Sensors, vol. 10, no. 12, pp.10506-10523, 2010.

[4] Pawar, A., Divya, K., "Secure and Efficient Data Transmission in Cluster based Wireless Sensor Network. International Journal of Computer Science and Mobile Computing," IJCSMC, vol. 4, no. 8, pp.132-142, 2015.

[5] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," IEEE Trans. Wireless Commun., vol. 1, no. 4, pp. 660-670, 2002.

[6] Mylsamy, R. and Sankaranarayanan, S., "A preference-based protocol for trust and head selection for cluster-based MANET," Wireless Personal Communications, vol. 86, no. 3, pp.1611-1627, 2016.

[7] Elhoseny, M., Elleithy, K., Elminir, H., Yuan, X. and Riad, A., "Dynamic clustering of heterogeneous wireless sensor networks using a genetic algorithm towards balancing energy exhaustion," International Journal of Scientific & Engineering Research, vol. 6, no. 8, pp.1243-1252, 2015.

[8] Hiremath, P. S., Anuradha, T. and Pattan, P., "Adaptive fuzzy inference system for detection and prevention of cooperative black hole attack in MANETs," International Conference on Information Science (ICIS), pp. 245-251, 2016.

[9] Su, Ming-Yang, "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems", Computer Communications, vol. 34, no. 1, pp. 107-117, 2011.

[10] Huang Lu, Jie Li, Kameda, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using ID-Based Digital Signature" in H.Global Telecommunications Conference (GLOBECOM 2010), pp. 1-5, 2010.

[11] Bhasker, L., "Genetically derived secure cluster-based data aggregation in wireless sensor networks," IET Information Security, vol. 8, no. 1, pp.1-7, 2014.

[12] Vasala, U., and Sakthidharan, G. R., "Effective Key Management in Dynamic Wireless Sensor Networks," International Journal of Computer Engineering In Research Trends, vol. 4, no. 7, pp. 308-312, 2017.

[13] Halford, T.R., Courtade, T.A., Chugg, K.M., Li, X. and Thatte, G., "Energy-efficient group key agreement for wireless networks," IEEE Transactions on Wireless Communications, vol. 14, no. 10, pp. 5552-5564, 2015.

[14] Shanmugam, K., Vanathi, B., Raja, R. and Priyanka, A., "Secure and efficient data transmission in wireless sensor network using set protocols", IJEDR NC3N, vol. 3, no. 2, pp. 1-7, 2015.

[15] Elhoseny, M., Elminir, H., Riad, A. and Yuan, X., "A secure data routing schema for WSN using Elliptic Curve Cryptography and homomorphic encryption," Journal of King Saud University-Computer and Information Sciences, vol. 28, no. 3, pp. 262-275, 2016.

[16] Pereira, N.C., Bastos-Filho, C.J. and de Moraes, R.M., "Improving AODV Route Recovery Mechanisms with Connectivity and Particle Swarm Optimization," Journal of Communication and Information Systems, vol. 27, no. 1, pp. 15-21, 2012.

[17] Singh, G., Kumar, N., and Verma, A.K., "Antalg: An innovative aco based routing algorithm for manets", Journal of Network and Computer Applications, Vol.45 pp.151-167, 2014.

Ms. Arudra Annepu, working as an assistent professor in Computer Science & Engineering Department at the Rajiv Gandhi Institute of Technology, Bagalore, affiliated to VTU. She received her Bachelors of Technology from Raghu Engineering College Visakhapatnam affiliated to JNTU and M.Tech from Andhra University. Her research interests are mobile computing, ad-hoc and wireless sensor networks.

Dr. M Jayaprasad received UG from BDT College of engineering, davanagere,in computer science & engineering. PG from bits pilani and Ph.D from Dr.M.G.R University and his area of research is network security. He has 27 years of

teaching experience. He worked various capacities like professor,vice-principal, principal in various technical organizations.He is Currently working as rector in Rajiv Gandhi Institute of Technology, Bagalore.