Received: November 3, 2018

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Energy Efficient Clustering Technique Using K-Means and AODV-ACO Routing with Secured AES Cryptography in MANET

Kavikondala Praveen Kumar Rao[1]* **Tamilarasan Senthil Murugan[1]**

[1]*Department of Computer Science & Engineering,*
Vel Tech Rangarajan Dr Sagunthala R & D Institute of Technology and Science, Avadi, Chennai, India
* Corresponding author's Email: praveenkumarrao.k@aol.com

Abstract: Mobile Ad-hoc Network (MANET) dynamically designed by the self-organization of the mobile nodes connected through wireless links without using any centralized administration. Energy consumption is the most significant issue in the MANETs, because most of the mobile host's functions have inadequate battery resources. Reduction in the energy consumption increases the lifetime and throughput of the network. The performance of existing techniques is less in terms of energy conservation issues. To overcome this limits, this paper suggested an energy conservation mechanism incorporated with a pro-active MANET routing scheme. The routing schema is employed in the energy level and the movement of the nodes. Calculation of energy cost is accomplished based on the assessment of the energy consumption level of the node, using K-Means clustering along with AODV (Ad-hoc On Demand Distance Vector). The data packets are secured using (AES), while sending data from source to destination. The proposed methodology "K-Means-AODV-ACO-AES" model is compared with the existing Optimal Key Management for Secure Data Transmission (OKMSDT) and Secured AODV (Sec-AODV). From the comparison result, it is observed that the K-Means-AODV-ACO-AES" increases in Packet Delivery Ratio (5%), along with the decrease in end-to-end-delay (6%), and energy consumption (7%) and drop (8%) in secured environment.

Keywords: Ad-hoc on demand distance vector, Centralized administration, End-to-end delay, Mobile ad-hoc network, Packet delivery ratio, Secure data transmission.

1. Introduction

MANETs is one sort of self-designing and dynamic remote system, which is self-possesses of several portable user equipment. The enhanced cluster maintenance scheme is essentially centered on limiting Cluster Head (CH) changing procedure with Least Cluster Head Change (LCC) and Cluster Based Routing Protocol (CBRP) [1]. Improved cluster maintenance scheme (ICMS) focused on minimizing frequency of CH changing process. Collection of new CH created on the simulation factor of CH and delayed time. ICMS performs better overhead in case of different range of speed and pause time for all mobile nodes [2]. The Blackhole attack causes reduction in packet delivery and packet drop/packet loss. The safe route between sending node and receiving node is accomplished by utilizing proficient AODV by increasing high packet delivery and receiving packet drop [3]. Clustering in WSN is performed to minimize the energy consumption and to reduce the data transmission over the network that is required to transmit the message to the base station. The CH becomes responsible for communication, which results into prolonged network lifetime [4]. Adaptive Fuzzy Interference System counteract and distinguish the black hole on MANETs. The adaptive method gives better performance in terms of throughput, end-to-end delay and packet delivery ratio in ad-hoc networks. The adaptive fuzzy logic system shows better performance compared to normal adaptive method [5]. MANET is extensively used in military purpose, a misadventure/ disaster area, Personal Area Network (PAN) and so on. The security features of communication among the nodes not performed. [6]. The IDS nodes must be set in sniff mode to perform Anti-Black-hole Mechanism

DOI: 10.22266/ijies2019.0630.28

(ABM) function. The IDS nodes are deployed in MANETs to detect and prevent selective Black-hole Mechanism. The network lifetime based on the different parameters based on the first and last node die but some fitness threshold statistic are not mentioned [7]. A Maximally Spatial Disjoint Multipath (MSDM) routing protocol is projected that is modified from Ad-hoc On-demand Multi Path Distance Vector (AOMDV) protocol. MSDM detects paths that spatially separated and maximally disjoint, so the energy consumption is less. The protocols may incur frequent route discovery requests if the topology is very dynamic. [8].

If the trust level does not meet the packet's requirement level, at that point the recipient must accomplish certain packet's necessity level before a node forwards a packet. The delay caused by security is much contrasted with the aggregate delay of a packet for large and inadequately associated networks. If the trust-level does not meet the packet requirements, the nodes need to play out a security affiliation like reconfirmation. Trust values decay with time and a security associated is triggered if the trust level is low [9]. Clustering is an efficient and analytical way to solve the secured critical problems in Wireless Sensor Networks (WSNs). The Secure and Efficient Data Transmission Identity-based digital signature (SET-IBS) and Identity-based online/offline digital signature Protocols (SET-IBOOS) are not varied with the speed/rate for better performance in sensor networks [10]. A lightweight dynamic channel distribution mechanism and an agreeable load balancing technique are appropriate for cluster based MANETs for enhancing execution in terms of throughput, energy consumption and Inter Packet Delay Variation (IPDV). The effects of upper layers such as the routing layer but instead focused on the MAC layer capability and local broad-casting services [11]. A framework for reliable multicast transmission using Time Division Multiple Access (TDMA) based channel access to Multicast Spanning Tree (MST) at the base station. The TDMA-based Reliable multicast MAC (TRM-MAC) protocol is used to sense the trade-off between delay performance and reliability. The performance of multicast improves the end-to-end reliability using TDMA-based reliable multicast MAC TRM-MAC protocols at the transport layer and the link layer. The algorithm didn't provide more speed and transmission rate in the simulation [12]. Multi-cast security in MANET utilized between the group correspondence and re-keying method for decreasing overhead and calculation cost. Time complexity is more in generating, distributing and updating keys [13]. The collaborative attack prevention protocol (routing) is employed in Secure Communication AODV (SCAODV). The AODV routing protocol is used to identify black hole attacks in MANETs. The performance of SCAODV is good, compared to the SAODV Protocol. The group of attackers is not addressed in the route. [14]. Adaptive Weighted Clustering Algorithm for mobile-ad-hoc network is used for maintaining the lifetime of nodes and discover the proper path between source and destination. The user must fit his needs and to take into consideration among different MANETs [15]. To overcome the above mentioned problems the, "K-Means-AODV-ACO-AES" is used for maintaining energy in the ad-hoc networks by enhancing QoS Parameters along with providing secured path to the destination. K-Means is used for clustering. AODV routing protocol is used for routing and that route is optimized using ACO techniques for choosing optimal path. Therefore, "K-Means-AODV-ACO-AES" methodology is used for enhancing parameters such as end-to-end-delay, Packet delivery ratio, energy consumption, and drop.

The rest of this paper is organized as follows: Section 2, reports on related-work. Section 3, presents a review on "K-Means-AODV-ACO-AES" Methodology in MANET. Section 4, describes the specification details of overall "K-Means-AODV-ACO-AES" methodology.

2. Literature survey

C. Aghi, and C. Diwaker [16] introduced the self-organization of nodes in the networks based on security using AODV in MANET. The trust based routing protocol was used for performing trusted routing discovery with cryptographic schemes at every routing protocols. A public key verification mechanism like certificate based authentication is needed, for the improvement of Trust based AODV (TAODV), in order to confirm the binding between the node's identity and its public key. The work is more complex in design and produce more overhead.

A. Bhatia, and R. C. Hansdah [17] implemented Bi-directional Multicast RPL Forwarding (BMRF) for low power and lossy Networks (RPL) multicast. A new multipath protocol called bi-directional multicast protocols is used for minimizing the amount of delivery delay and send packets, which has small memory usage. The protocols are configurable in order to trade off energy consumption, reliability, and latency. The contention between feedback messages sent by the receivers of a multicast packet is not efficient.

A. Dhaka, A. Nandal, and R. S. Dhaka [18] presented a new method for black-hole node detection based on the control sequence. Here, the routing protocol sent the control sequence to its neighboring nodes and each individual node response assembly decides whether that node is a malicious node or not. In this, Packet Delivery Ratio (PDR) increased with less overhead in routing. The misbehaving nodes can more drop packets being accused and isolated from the network during the preliminary phase.

D. Garg, and P. Gohil [19] introduced a novel routing algorithm for MANETS based on the swarm intelligence. This research used Ant Colony Optimization (ACO) algorithm for optimal path selection. Maintenance of the route has to be done occasionally with the selected optimal path for data transmission but security criteria not discussed.

G. Singh, N. Kumar, and A. K. Verma [20] have suggested an innovative ACO based Routing Algorithm (ANTALG) by considering an irregular selection of source and destination nodes and exchanges the Ants (agents) between them. Here this algorithm was associated with the AODV, Ant Dynamic Source Routing (ADSR), and Hybrid Ant Colony Optimization Routing Algorithm (HOPNET), which showed that the proposed algorithm delivered good throughput and reduced end-to-end-delay, packet drop, average jitter but security features were not deliberate. The security features for communication among the ants in MANETs should be further enhanced.

M. Anupama and B. Sathyanarayana [21] designed an Optimal-Key-Management technique for Secure Data-transmission (OKMSDT) in MANETs. The authenticating and key distribution was used to monitor symmetric-key among gatherings. The signal strength dispersion the link-stability metric to a path rating metric appears capable in ad-hoc networks.

J.A.D.C Anuradha, R. Samarasinghe and S.R. Kodituwakku [22] implemented light weighted authentication secure routing protocol on the top of an AODV. The authentication with integrity is to be further developed and diminish the number of messages send over the large-scale networks.

3. K-means-AODV-ACO-AES methodology

The “K-Means-AODV-ACO-AES” is used for maintaining the energy in Ad-hoc Networks by enhancing End-to-End delay, throughput, Packet delivery ratio, Energy consumption, Routing overhead and Packet Drop. The security is the key concern in any of wireless network. Advanced Encryption Standard (AES) is used to avoid security disputes in the complete network. AODV routing protocol is used for efficient route establishment, when there is a demand for new route in the network. ACO is used for enhancing the AODV. In this work, K-Means-AODV-ACO-AES methodology consists of four steps: i) Organization of sensor-nodes ii) Grouping/clustering of different-networks iii) Routing process starts iv) Secure transmission using AES.

3.1 Initial deployment/organization of ad-hoc nodes

The ad-hoc nodes randomly deployed in a region of the ad-hoc-networks. In each Sensor Node (SNs), the id and positions are analyzed and identified, when the node delivers the data through the network. The information delivered through the network and data is encrypted using AES encryption for delivering the confidential information. Next, clustering/grouping of sensor nodes take place using K-Means Clustering.

3.2 Clustering algorithm using K-means

The clustering algorithm minimizes the communication in a local domain and communicate through forwarding nodes (gateway nodes). A group of nodes forms a cluster and the local interactions among cluster members organize through a CH. The clustering techniques of networks described in the following steps.

A k number of clusters generated from the n number of SNs, the fitness function is minimized by the calculation. The fitness function that is utilized in this k-means clustering is squared error function and it is given in Eq. (1).

$$F = \sum_{j=1}^{k} \sum_{i=1}^{n} \left\| x_i - c_j \right\|^2 \qquad (1)$$

Where, the center of j^{th}cluster is represented as c_j, data point of i^{th} sample is denoted as x_i and the distance from each SN to the cluster center is represented by $\left\| x_i - c_j \right\|^2$.

There are four important steps performed in K-means clustering algorithm.

Step 1:

In the beginning, the k clusters are originated from the SNs by taking the k number of centroids at random places.

Step 2:

Received: November 3, 2018

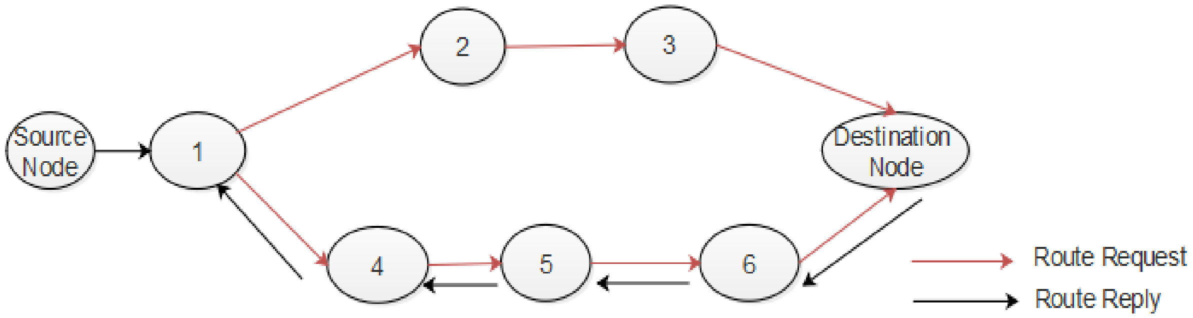

Figure. 1 AODV routing protocols-data transfer

The Euclidean distance from each SN to the centroid is computed for making the k initial clusters. Consider each node is closest to the centroid. The Euclidean distance from one node to another node is given in Eq. (2).

$$Eucildean\ distance = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2} \quad (2)$$

Where, the co-ordinates of x and y axis is represented as x_1, x_2 and y_1, y_2 respectively.

Step 3:

The position of each node is verified from the previous position and the each-cluster locations are again generated in a networks.

Step 4:

If the locations of centroid changes, then again step 2 should be processed for creating the effective clusters or else the grouping process needs to be ended. Finally, the centroid which is selected from the K-means clustering is considered as an optimum CH for a cluster group. After clustering of the network, routing process takes place using AODV Routing-protocol and optimized using ACO techniques.

3.3 AODV-routing protocol

The routing protocol is projected for mobile nodes in an ad hoc network. The AODV is calculated to reduce the distribution of overhead and control traffic. The AODV protocol deals with two functions such as Route Discovery and Route Maintenance. The finding of the fresh route predicts 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 preserve permanent route Table. AODV is rapidly able to analyze the changes in network topology. The Data transfer of AODV is given in Fig. 1. AODV Routing Protocol is optimized using ACO techniques.

3.4 ACO technique

The ACO routing optimization algorithm takes interest from the attributes of ants in nature and from the related field of ACO to determine the issues of routing in ad-hoc networks. The important source of inspiration found in the capacity of specific kinds of ants to look through the shortest path between their nests and food sources utilizing Pheromone (Impulsive Chemical Substance). Insect leave hints of pheromone as it moves between sources to destination. Ants specially go in the course of high pheromone concentrations in search of food. The higher levels of pheromone received, when lowest paths complete faster. The positive establishment procedure allows the colony to address the shortest path. The data are encrypted and decrypted using AES Cryptography.

3.5 AES encryption

AES algorithm is used for the security as well as it improves the speed. This AES encryption transforms the information into unintelligible form named as cipher text and it has ten rounds of encryption. Each round has four processing steps such as sub-bytes, shift-rows, mix column and add round key. The process of AES encryption is shown in Fig. 2 that is explained below.

3.5.1. Sub bytes

In each-byte of the state, a non-linear-byte-substitution of sub bytes transformation is independently operated by employing the substitution Table. In that table, each individual byte represents by new byte such as the row value is the leftmost 4-bits of the byte and the column value is right most 4-bits of the byte. In that substitution table, these rows and column values are transported the indexes and it is used for choosing the 8-bit unique code.

3.5.2. Shift rows

The first rows of a state are not modified in a shift rows transformation. 1-byte circular left-shift is executed for a second row and 2-byte circular left-shift is accomplished for a third row and in fourth row 3-byte round left-shift is executed. Shift row transformation is more suitable for an array of 4-byte columns treating the cipher input and output.

3.5.3. Mix columns

Individually on each column, the mix column transformation is accomplished. A new column is generated based on each column, which is a function of all 4-bytes in that column.

3.5.4. Add round key

In add round key transformation, only one column proceeds at the time of execution and the bits of the state are XORed (add round key operation) output with the bits of round key. It is found in column wise operations concerning the 4-bytes of state column and to the single word of the round key and in addition, it is viewed as byte level activity.

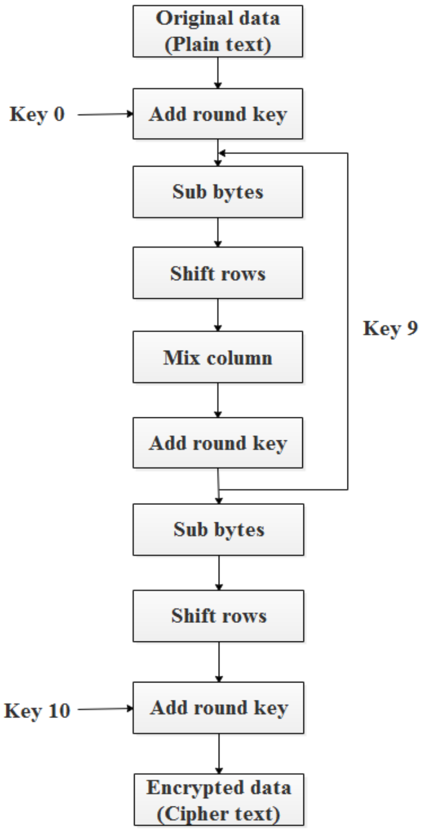

Figure. 2 Flowchart of AES encryption

3.6 AES decryption

AES decryption extracts plain text (original form) from the cipher text, which is generated by the AES encryption. This AES decoding is refined by turning around all means of AES encryption with inversing capacities; for example, opposite move lines, backwards substitute bytes, including round key, and converse blend segments. Inverse substitute bytes have XOR output (add round key operation) of preceding two steps with four words from the key schedule and the inverse mix columns does not undergo the decryption process. The process of AES decryption is shown in Fig. 3.

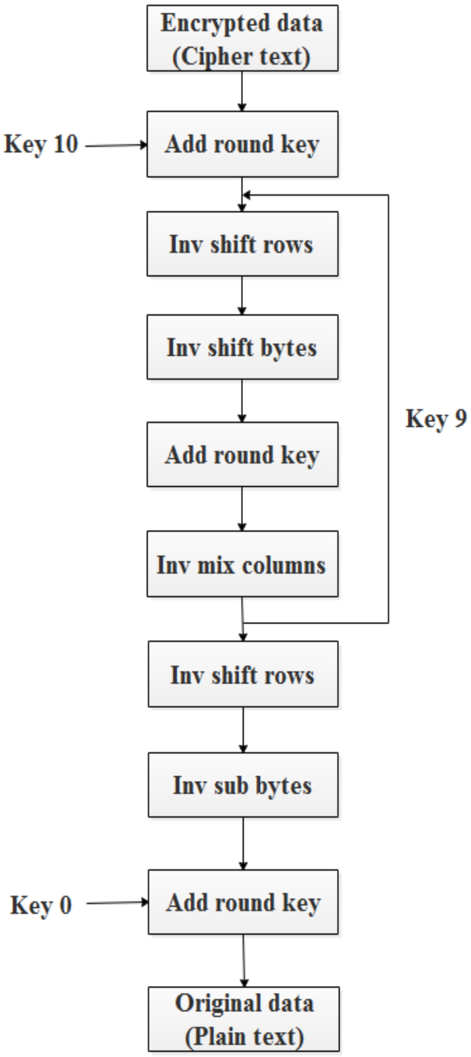

Figure. 3 Flowchart of AES decryption

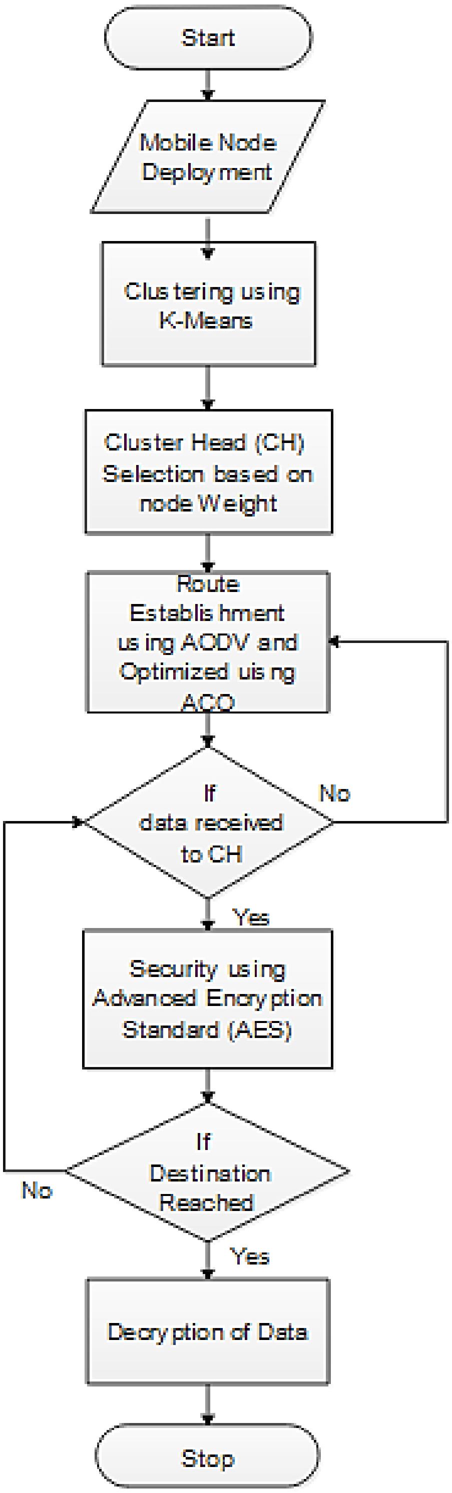
Start
Mobile Node Deployment
Clustering using K-Means
Cluster Head (CH) Selection based on node Weight
Route Establishment using AODV and Optimized using ACO
If data received to CH
No
Yes
Security using Advanced Encryption Standard (AES)
If Destination Reached
No
Yes
Decryption of Data
Stop

Figure. 4 Flow chart of overall method

The Fig. 4 shows a flow chart of overall methods discussed above. First, deployment of mobile nodes is organized. Then, the dynamic clustering method uses K-Means for solving the problem in finding a longest path for transmitting data. Based on the minimum value of degree, the cluster head is chosen in the network. The route discovery and route maintenance for routing using AODV Routing Protocol established and optimized using ACO Techniques. The encryption and decryption of transmission data performed using an AES Cryptography algorithm. Thus, "K-Means-AODV-ACO-AES" method gives better results in terms of End-to-End delay, throughput, Packet delivery ratio, Energy consumption, Routing overhead and Packet Drop.

4. Experimental results

The "K-Means-AODV-ACO-AES" method is implemented in the NS2 simulation tool. The simulation parameters are shown in Table 5. The simulation starts and end time are denoted as 0.0001-50.0000 secs respectively by varying the number of static nodes as 20, 40, 60, 80 and 100. The MAC Type is 802_11 with Omni Antenna model. This section gives a detailed view of the results that are obtained using "K-Means-AODV-ACO-AES" provides energy efficient and secured routing while transmitting data from source to destination by giving better performance compared to the OKMSDT [21] and SecAODV [22]. The Performance is calculated by measuring the delay, delivery ratio, energy consumption and drop parameters. The performance metrics is given below.

4.1 Packet-delivery-ratio

Based on a total amount of packets established in a ratio by a total number of destination packet sent by the source node is given in Eq. (3)

$$DelRatio = \frac{(no.of\ packets\ send - packets\ lost)}{no.of\ packets\ send} \times 100 \quad (3)$$

4.2 Energy consumption

The huge number of nodes is equivalent to the huge amount of received energy consumption. A node drops a specific amount of energy for every packet transmission and received, which is given in Eq. (4)

$$Energy = \frac{amount\ of\ energy\ for\ every\ packets}{total\ simulation\ time} \quad (4)$$

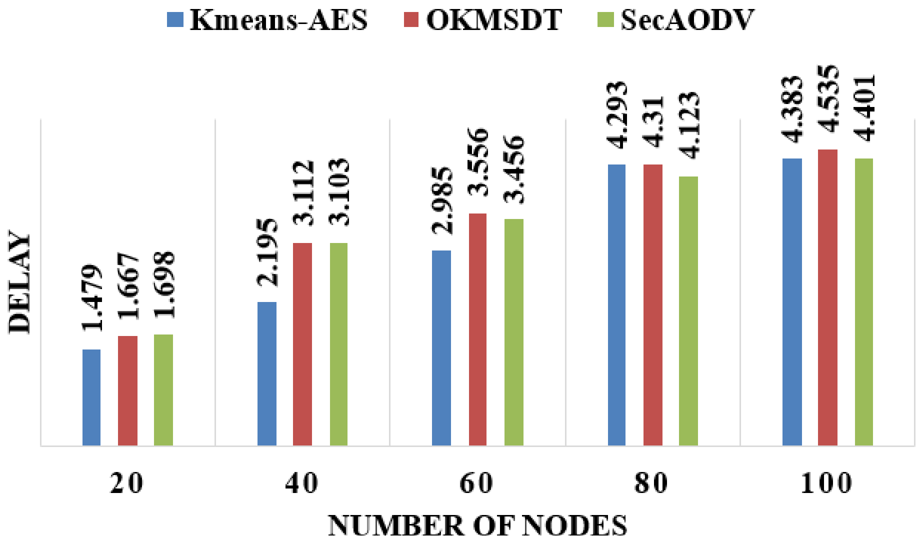

Figure. 5 Nodes vs. delay

Table 1. Number of nodes vs. delay

QoS	Delay				
Nodes	**20**	**40**	**60**	**80**	**100**
OKMSDT [21]	1.667	3.112	3.556	4.31	4.535
SecAODV [22]	1.698	3.103	3.456	4.123	4.401
K-means –AES	1.479	2.195	2.985	4.293	4.383

Table 2. Number of nodes vs. DelRatio

QoS	DelRatio				
Nodes	**20**	**40**	**60**	**80**	**100**
OKMSDT [21]	100.67	216.37	235.35	250.05	300.73
SecAODV [22]	98.69	209.98	215.56	236.06	266.45
Kmeans -AES	197.75	237.38	265.35	289.95	310.75

4.3 Delay

The difference between sending time of packets and receiving time of packets is known as delay, which is given in Eq. (5).

$$Delay = Time\ spend\ on\ Hop1 + time\ spend\ on\ Hop2 + \cdots .. + time\ spend\ on\ Hop\ n \quad (5)$$

4.4 Packet drop/packet loss

The total amount of packets sends and packet established is known as the packet drop/packet loss, which is given in Eq. (6).

$$Drop = \frac{(Total\ no.of\ packets\ send\ (ps) - Packet\ received(pr))}{Total\ number\ of\ simulation(s)} \quad (6)$$

Table 1 shows the delay by changing different nodes 20, 40, 60, 80, and 100 of fixed Nodes. Hence, K-Means-AODV-ACO-AES" Methodology shows better results than OKMSDT and Sec-AODV.

The Evaluation of Nodes vs. delay between Kmeans-AES and existing method is plotted in Fig. 5. The delay value is decreased in K-means-AES method compared to the OKMSDT and Sec-AODV method with different 20, 40, 60 80 and 100 Nodes.

Table 2 shows the DelRatio by changing different nodes such as 20, 40, 60, 80, and 100 of fixed Nodes. Hence, K-Means-AODV-ACO-AES" Methodology shows better results compared to OKMSDT and Sec-AODV.

The Evaluation of Nodes vs. DelRatio between Kmeans-AES and existing method is plotted in Fig. 6. The DelRatio value is increased in Kmeans-AES method compared to the OKMSDT and Sec-AODV method with different 20, 40, 60 80 and 100 Nodes.

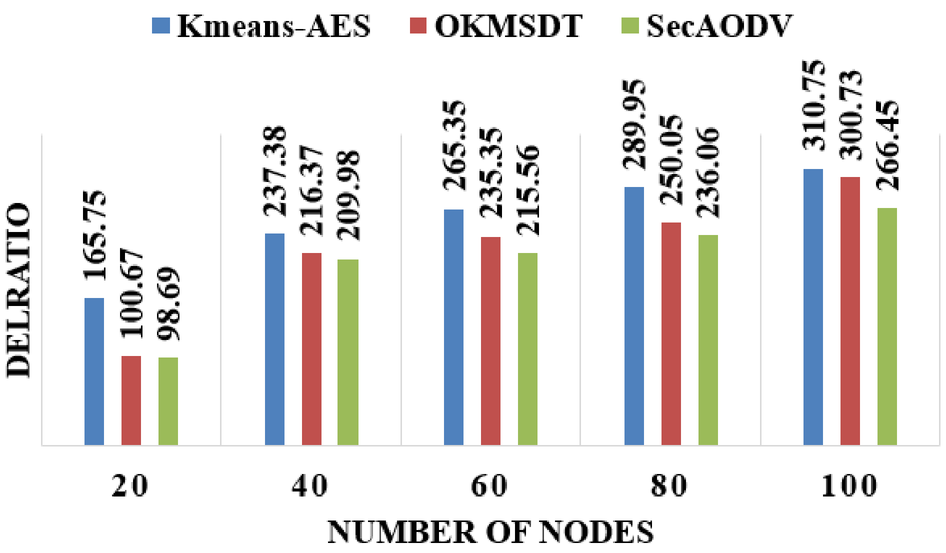

Figure. 6 Nodes vs. DelRatio

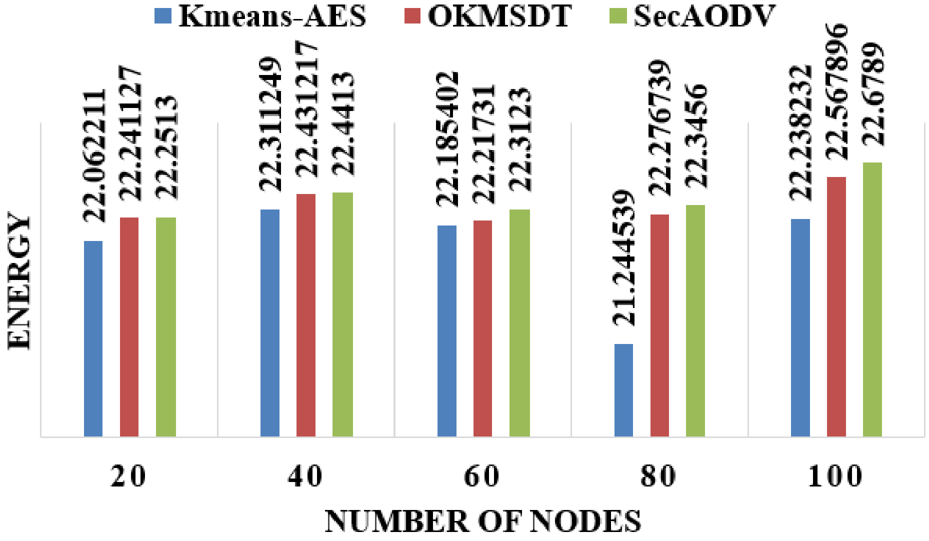

Figure. 7 Nodes vs. energy

Table 3. Number of nodes vs. energy consumption

QoS	**Energy Consumption**				
Nodes	**20**	**40**	**60**	**80**	**100**
OKMSDT [21]	22.24113	22.43122	22.21731	22.17674	22.5679
SecAODV [22]	22.2513	22.4413	22.3123	22.3456	22.6789
Kmeans -AES	22.062211	22.31124	22.18540	21.97453	22.23823

Table 3 shows the Energy consumption by changing different nodes such as 20, 40, 60, 80, and 100 of fixed Nodes. Hence, K-Means-AODV-ACO-AES" Methodology shows better results than OKMSDT and Sec-AODV.

The Evaluation of Nodes vs. Energy Consumption between Kmeans-AES and existing method is plotted in Fig. 7. The Energy consumption value is decreased in Kmeans-AES method compared to the OKMSDT and Sec-AODV method with different 20, 40, 60 80 and 100 Nodes.

Table 4. Number of nodes vs. drop

QoS	Drop				
Nodes	**20**	**40**	**60**	**80**	**100**
OKMSDT [21]	22.241127	22.431217	22.21731	22.1767	22.5678
SecAODV [22]	689	756	856	967	987
Kmeans –AES	22.062211	22.311249	22.18540	21.97453	22.2382

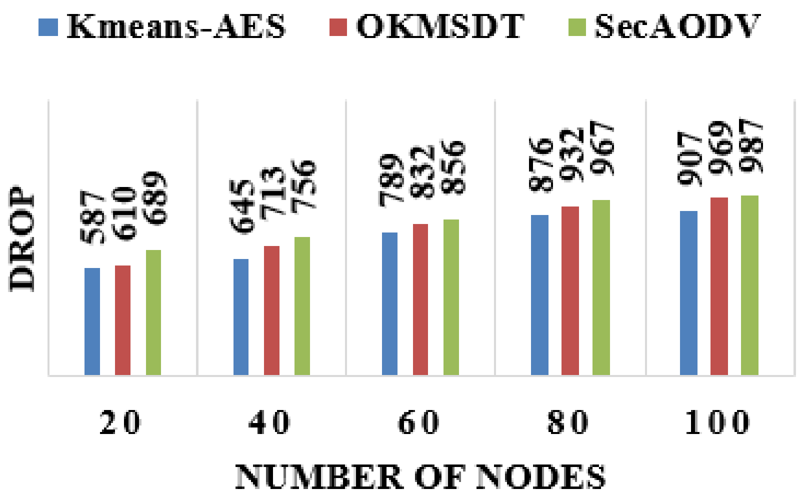

Figure. 8 Nodes vs. DelRatio

Table 5. Simulation parameters

Clustering Algorithm	K-Means
Routing Protocol	AODV
Security	AES
Simulator Tool used	NS2
Simulation start time	0.0000000001
Simulation End time	50.000000000
Number of mobile nodes	20, 40, 60, 80 and 100
Antenna Model	Omni Antenna
Minimum speed	28 ms
Network Interface types	Wireless
MAC Type	MAC/802_11
Initial Transmit Power	0.660
Initial Receive Power	0.395

Table 4 shows the drop by changing different nodes such as 20, 40, 60, 80, and 100 of fixed Nodes. Hence, K-Means-AODV-ACO-AES" Methodology shows better results than OKMSDT.

The Evaluation of Nodes vs. drop between Kmeans-AES and existing method is plotted in Fig. 8 the drop value is decreased in Kmeans-AES method compared to the OKMSDT and Sec-AODV method with different 20, 40, 60 80 and 100 Nodes.

The "K-Means AODV-ACO-AES" methodology provides energy efficient routing over mobile ad-hoc networks in very efficient way by securing data packets from source to destination. The simulation parameters are shown in Table 5 in section 4.5. Hence, the simulation start and end time are as 0.001-50.00 ms respectively with minimum speed 28ms by using Omni antenna. The 802_11 wireless MAC is used with initial transmit power 0.660.

4.5 Specification

Table 5 shows the simulation parameters.

5. Conclusion

This section describes the conclusion of the proposed energy conservation mechanism. The energy cost is considered based on the prediction of the energy consumption level of the node. The energy cost computation performed using the K-means clustering along with the AODV routing and AES cryptography for securing data. The "K-means-AES" model handles network state related constraints like energy consumption of node and secured routing path in the ad-hoc networks. The performance of the proposed "K-Means-AODV-ACO-AES" model is compared with the existing OKMSDT and Sec-AODV models. The proposed model achieved better results in increasing Packet delivery ratio (5%), with decrease in end-to-end delay (6%), drop (8%) and energy consumption (7%) with secured routing in ad-hoc networks than OKMSDT and Sec-AODV methodology. Enhancement of any hybrid methodology in the security related processes of the ad-hoc networks could be done in the future for further improvement.

References

[1] S. Pathak and S. Jain, "A novel weight based clustering algorithm for routing in MANET", *Wireless Networks*, Vol.22, No.8, pp. 2695-2704, 2016.

[2] S. Pathak, N. Dutta, and S. Jain, "An improved cluster maintenance scheme for mobile AdHoc networks", In: *Proc. of IEEE International Conf. On Advances in Computing, Communications and Informatics*, pp.2117-2121, 2014.

[3] N. Jaisankar, R. Saravanan, and K.D. Swamy, "A novel security approach for detecting black hole attack in MANET", In: *Proc. of IEEE International Conf. on Information processing and management*, pp.217-223, 2010.

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

[5] P.S. Hiremath, T. Anuradha, and P. Pattan, "Adaptive fuzzy inference system for detection and prevention of cooperative black hole attack in MANETs", In: *Proc. of IEEE International Conf. On Information Science*, pp.245-251, 2016.

[6] J.L. Burbank, P.F Chimento, B.K. Haberman, and W.T. Kasch, "Key challenges of military tactical networking and the elusive promise of MANET technology", *IEEE Communications Magazine*, Vol.44, No.11, 2006.

[7] M. Elhoseny, K. Elleithy, H. Elminir, X. Yuan, and A. Riad, "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] W. Almobaideen, R. Al-Soub, and A. Sleit, "MSDM: Maximally Spatial Disjoint Multipath Routing Protocol for MANET", *Journal of Communications and Network*, Vol.5, pp.316-322, 2013.

[9] D.Q. Nguyen, M. Toulgoat, and L. Lamont, "Impact of trust-based security association and mobility on the delay metric in MANET", *Journal of Communications and Networks*, Vol.18, No.1, pp.105-111, 2016.

[10] H. Lu, J. Li, and M. Guizani, "Secure and efficient data transmission for cluster-based wireless sensor networks", *IEEE Transactions on Prallel and Distributed Systems*, Vol.*25*, No.3, pp.750-761, 2014.

[11] B. Karaoglu and W. Heinzelman, "Cooperative load balancing and dynamic channel allocation for cluster-based mobile ad hoc networks", *IEEE Transactions on Mobile Computing*, Vol.14, No.5, pp.951-963, 2015.

[12] C.G. Lorente, B. Lemmens, M. Carlier, A. Braeken, and K. Steenhaut, "BMRF: Bidirectional Multicast RPL Forwarding", *Ad Hoc Networks*, Vol.54, pp.69-84, 2017.

[13] V. Rajamanickam and D. Veerappan, "Inter cluster communication and rekeying technique for multicast security in mobile ad hoc networks", *IET Information Security*, Vol.8, No.4, pp.234-239, 2014.

[14] S. Sharma, U.K. Singh, K.C. Phuleriya, and D.N. Goswami, "SCAODV: A Protocol to Prevent Black Hole Attacks in Mobile Ad Hoc Networks", *International Journal of Computer Science & Communication*, Vol.6, No.2, pp.36-41, 2015.

[15] A. Yasin and S. Jabareen, "Adaptive Weighted Clustering Algorithm for Mobile Ad-hoc Networks", *International Journal of Computer Network and Information Security*, Vol.8, No.4, p.30, 2016.

[16] C. Aghi and C. Diwaker, "Black hole attack in AODV routing Protocol: A review", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol.3, No.4, pp.820-823, 2013.

[17] A. Bhatia and R. C. Hansdah, "TRM-MAC: A TDMA-based reliable multicast MAC protocol for WSNs with flexibility to trade-off between latency and reliability", *Computer Networks*, Vol.104, pp.79-93, 2016.

[18] A. Dhaka, A. Nandal, and R. S. Dhaka, "Gray and Black Hole Attack Identification Using

Control Packets in MANETs", *Procedia Computer Science*, Vol.54, pp.83-91, 2015.

[19] D. Garg and P. Gohil, "Ant Colony Optimized Routing for Mobile Ad Hoc Networks (MANET)", *International Journal of Smart Sensors and Ad Hoc Networks*, Vol.2, No.3, pp. 4, 2012.

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

[21] M. Anupama and B. Sathyanarayana, "An Optimal Key Management Technique for Secure Data Transmission in MANET", *Journal of Theoretical & Applied Information Technology*, Vol.95, No.16, pp.3783-3795, 2017.

[22] J.A.D.C.A. Jayakody, R. Samarasinghe, and S.R. Kodituwakku, "SecAODV: Lightweight Authentication for AODV Protocol", *International Journal of Computer Applications*, Vol.137, No.13, pp.33-38, 2016.