International Journal of Pure and Applied Mathematics
Volume 117 No. 21 2017, 631-649
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

Efficient and Secure Data Transmission in MANETs against Malicious AttackUsing AODV Routing and PSO Clustering with AES Cryptography

[1]Md. Sameeruddin Khan and [2]Md. Yusuf Mulge

[1]Computer Science & Engineering,

Rayalaseema University, Kurnool, A.P.

sameerirfan70@gmail.com

[2]Dept. of Computer Science and Engineering,

CVR College of Engineering,

Rangareddy (D), Telangana.

dryusufmulge@gmail.com

Abstract

Mobile Ad-Hoc Network (MANET) is a self-configuring network of mobile nodes linked by wireless creating a random topology. The nodes are free to move randomly. Thus, the network's wireless topology may be haphazard and may alter rapidly. The efficient route is established using AODV Routing Protocol. The Particle Swarm Optimization (PSO) algorithm is used for clustering of sensor nodes and maintaining load balancing in efficient way.Efficient black hole detection using Malicious Node Detection Mechanism-TX/RX (MNS-TX/RX) with optimized routing algorithm is implemented in secured environment by using Advanced AES cryptography. Thus "AODV-PSO-AES-MANETs" algorithm has precisely detect the black hole node and finds the proper solution for transmitting data for maintaining life-time and Load-balancing by analyzing performance such as,Through-put, routing overhead, packet delivery ratio, drop, delay and energy consumptionin secured environment.

Key Words: Advanced encryption Standard, ad-hoc on-demand distance vector routing, Black Hole Attack, mobile Ad-Hoc network, and particle swarm optimization.

1. Introduction

Mobile Ad-Hoc Network (MANETs) is one kind of self-configuring and dynamic wireless network, which is composed of several movable user equipment.Mobile nodes are communicated with each other without any fixed central base station to monitor the nodes and to transfer data between the nodes [1, 2].MANETs technologies includes system-level architecture, routing(both interior and exterior), security, medium access control (MAC) and management [3]. Black hole nodes is detected in this paper in an efficient way. The Blackhole attack is present with packet delivery and less packet drop/packet loss. The safe route between sending node and receiving nodeis achieved by using efficient AODV by increasing high packet delivery and reduce packet drop. A malicious node dropping all the traffic in the network, whichmakes use of the vulnerabilities of the route discovery packets of the on-demand protocols [4]. The intermediate nodes are responsible for finding a fresh path to the destination and sending discovery packets to the neighbor nodes in the route discovery process of AODV protocol [5]. Adaptive Fuzzy interference system to prevent and detect the supportive black hole attack on MANETs. The adaptive method increases through-put, end-to-end delay and packet delivery ratio. The adaptive fuzzy logic system shows better performance compared to normal adaptive method [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]. On-demand power-balanced routing algorithm for mobile and multi-hop networks is presented in this paper. The packet delivery ratio can be improved by controlling better-residual charge through the power-balanced algorithm [8]. A random selection of sourceand destination nodes exchange the ants (agents) to reduce average jitter compared with AODV, ADSR and HOPNET. ANTALG has better performance, when compared with HOPNET, ADSR and AODV [9].A bullet-proof verification (BPV) method is used to detect the blackhole attack, either signal or cooperative in mobile ad-hoc networks. The BPV method consist of two methods i) every node first examines suspicious node using local neighborhood information. ii)It send an encrypted (bullet-proof) test message to the destination, if node receives RREP from a suspicious node [10]. The collaborative attacks prevention routing protocols is used in this paper for secure communication AODV (SCAODV). The AODV is based on solution to mitigate black hole attacks in MANETs. The performance of SCAODV is good, when compared to theSAODV Protocol [11]. Black hole attackis one of the severe security threats in MANETs. Hence, this paper provide best way to identify malicious node by processing Route Request [12,20].

A fundamental security problemin MANET is used to protect basic functionality to deliver data bits from one node to another. Ant Colony Optimization is used to detect and prevent blackhole attack in MANETs in this paper. Themalicious

node can deprive the traffic from the source nodeby sending fake route reply [13]. A malicious node incorrectly sends the Route Reply (RREP)with minimum hop count to destination. AODV Routing protocol is reactive protocols used for detecting black-hole attacks in network. The routing process is not defined in this paper [14]. The malicious black hole attack is implemented in the network to measure throughput, delivery ratio, packet delivery and delay. The SAODV protocols provides only better through-put in network[15].

To conquer this problem, "AODV-PSO-AES-MANETs" is implemented for increasing the parameters such as, Through-put, Routing Overhead, Packet Delivery ratio, drop, delay and energy Consumption. In this work, the essential modification in AODV is used for the purpose of achieving the performance in the presence of black hole attack and find efficient routing path using PSO clustering to the desired destination. The black hole attack is predicated using MND-TX/RX Mechanism.The Advanced Encryption Standards (AES) is used in security and it communicates with another node for the secured communication. Thus, "AODV-PSO-AES–MANETs" method gives better results in through-put, Routing Overhead, Packet Delivery ratio, drop, delay and energy Consumption than existing method.

2. Related Work

Gurpreet Singh et.al has presented 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 performance parameterswere compared with the AODV, ADSR, and HOPNET, conclude that the proposed algorithm gives good throughput and reduced average end to end delay, packet drop, average jitter but security features were not discussed.

Dweepnagarg*et al.* [16] has introduced a novel routing algorithm for MANETS based on the swarm intelligence. In this, for optimal path selection, Ant Colony Optimization (ACO) algorithm has used. Maintenance route has to be done periodically, with this optimal path has selected for data transmission but security criteria are not discussed.

Arvind Dhaka et.al [17] has presented a new method for black hole node detection based on the control sequence. Here the control sequence has sent the control sequence to its neighboring nodes and depending each and individual node response making the decision whether that node is a malicious node or not. In this packet delivery ratio (PDR) has increased but the little overhead in routing.

Nishitha Taraka et.al [18] has demonstrated the scalability of Ant colony optimization based Ad hoc networks (AntHocNet) and done the comparison with AODV and DSR. AntHocNet performed better at high data rates with a large number of nodes but its performance is inferior to that of AODV and DSR at low data rates with less number of nodes. But a security criterion is not

discussed.

V. Manjusha et.al [19] has introduced the three different kinds of black hole detection schemes and has analyze all the three detection schemes by considering the energy consumption, throughput, and end to end delay. It gives the best results of throughput as well as energy consumption but here it has a limitation in delay and overhead.

3. AODV-PSO-AES-MANETsMethodology

The "AODV-PSO-AES-MANETs" is used to detect the malicious node, while transmitting data in the network. The security is the chief concern in any of wireless network.AdvancedEncryption Standard (AES) is used to avoid security issues in the complete network.AODV routing protocols are used for efficient route establishment, when there is a demand for a new route in the network. A black hole attack is known as malicious/false node, which waits for others nodes to Send Route Request (RREQ) messages. The blackhole attack is identified using MND-TX/RX. When the data is actually started transferring it absorbs all the packets and send to the destination. In this work, AODV-PSO-AES-MANET methodology consists of eight steps such as i) Deployment of Sensor Nodes ii) Groping/clustering of different networks iii) Routing process starts iv) Secure transmission using AES and Black-hole identification using Malicious Node Detection TX/RX (MND-TX/RX).

3.1. Clustering Algorithm Using K-means

The clustering algorithm limit the communication in a local domain and transmit the forwarding nodes (gateway nodes). A group of nodes form a cluster and the local interactions between cluster members are controlled through a CH. The following steps describes, how the clustering of networks takes place;

Ak number of clusters are generated from the n number of SNs, the fitness function is minimized by the algorithm. The fitness function which is used in this k-means clustering is squared error function and it is given in equation (1).

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

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

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

Step1: In the beginning, the k clusters are created from the SNs by taking the k number of centroids at random places.

Step 2: 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 equation (2).

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

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 areagain calculated in a network.

Step 4: If the position of centroid becomes changed, then again go to step 2 for obtaining the effective clusters else the clustering process to end.Finally, the centroid which is selected from the K-means clustering as an optimum CH for a cluster groups.

PSO is used for optimizing the different CH in the ad-hoc network.

3.2. Energy Efficient Clustering-Load balancing Using Particle Swarm Optimization (PSO)

PSO optimize the clustering, which yields motivation from the characteristics of ants in nature and from the related field of PSO to solve the issue in communicating networks for choosing shortest routing process. PSO is an optimization algorithm, which simulates the movement and flocking of birds. A particle swarm is a population of moving object, which can move through the search space and can be attracted to the better positions. Each bird is refers to as a "particle", which fly with a certain velocity and move to find the global best position. PSO is a global search algorithm, which has a strong ability to detect global optimistic results. The clustering is done using PSO in Ad-hoc network. Basic Clustering methods of sensor Nodes is given in Fig.1. Load balancing means to maximize throughput, minimize response time and routing overhead in the network. The clustering in sensor nodes has been widely pursued by the research community in order to solve the scalability, energy and life-time issues of sensor networks.

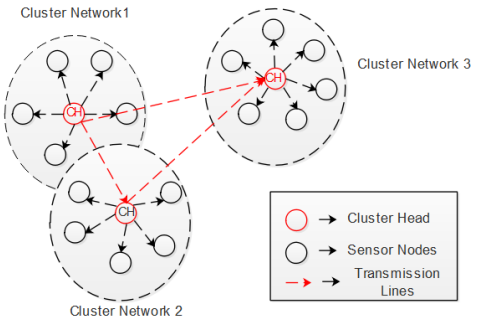


Fig.1: Basic Clustering Methods of Sensor Nodes

In Fig.4. 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.Given that the CHs' transmitters and receivers are calibrated, balanced and geographically distributed, clusters are created.Each node knows when it is its turn to transmit, according to the time slot schedule.The CHs collect messages from all their cluster members, aggregate these data, and send the result to the BS.

Cluster Head – A head node, which coordinate between same cluster member and another CHs is known as CH.

Cluster Members –The cluster members share information from sameCH in the same cluster networks.

3.3.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 byRoute 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 Fig.2

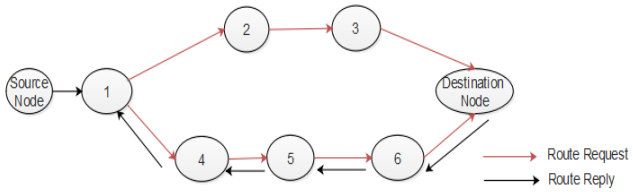


Fig.2: AODVRouting Protocols-Data Transfer

3.4. Advanced Encryption Standard (AES)

AES is a symmetric block cipher. The protocol design provides the non-repudiation, integrity, confidentiality, and authentication with AES method. The cryptographic algorithm with encryption method consists of both sender and receiver. Both sender and receiver share the common key value for encryption and decryption. The sender and receiver share common key value. The cryptographic algorithm analyses some secure way to provide encrypted and decrypted key the receiver. To deliver the key to the receiver, the effective key distribution is needed. The pair of keys for encryption is used. Every user has a single pair of keys. The public key can be accessed by any one. The private key

is a secret key, which is not known by any others. The AES algorithm requires less computational processing time and encrypt faster. The growth in key size, as well as block size and security,get enhanced. AES is based on the message recovery, which includes a message and the signature. AES is faster and stores data in compressed format.

i) AES Encryption

AES algorithm used for the security purpose as well as it improves the speed. This AES encryption transforms the information into unintelligible form named as ciphertext and also 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 rounds from one to nine is alike to the tenth round, which is eliminates the process of mix columns. The process of AES encryption shown in Fig 3. Which is explained below:

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 is represented by new byte such as the row value is a leftmost 4 bits of the byte and the column value is right most 4 bits of the byte. In that substitution table, these row and column values are delivered the indexes and it is used for electing the 8-bit unique code.

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 2^{nd} row and 2-byte circular left shift is executed for a 3^{rd} row as well as in fourth row 3-byte circular left shift is executed. Shift row transformation is more considerable for an array of four 4-byte columns treating the cipher input and output.

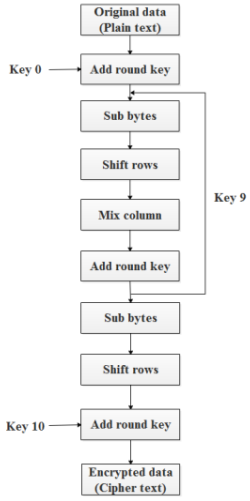


Fig. 3: Flowchart of AES Encryption

Mix Columns

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

Add Round Key

In add round key transformation, only one column proceeds at the time of execution and the bits of the stateare XORed (add round key operation) output with the bits of round key. It is explored in a column-wise operation among the 4 bytes of state column and to the one word of the round key as well as it is viewed as byte-level operation.

ii) AES Decryption

AES decryption is extracted plain text (original form) from the ciphertext, which is generated by the AES encryption. This AES decryption is accomplished by reversing all steps of AES encryption with inversing functions such as inverse shift rows, inverse substitute bytes, add round key, and inverse mix columns. Inverse substitute bytes have XOR output (add round key operation) of previous two steps with four words from the key schedule and the inverse mix columns do not commit into decryption process. The process of AES decryption shown in Fig 4.

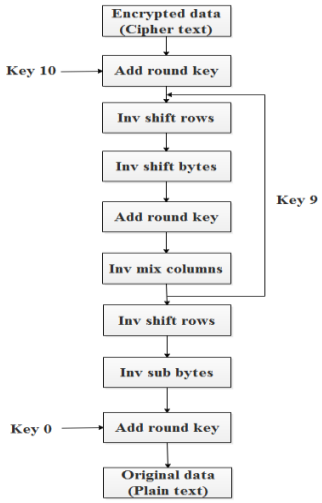
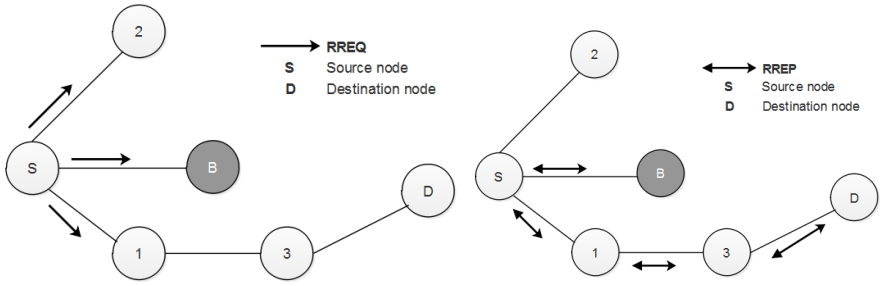


Fig. 4: Flowchart of AES Decryption

3.5. Black Hole Attack Detection

The false node responds to routing request with a large sequence number, least hop. The source node transmits data to the destination over the black-hole node. By this way, a black-hole node diverts most of a traffic of the network to itself and it drops the data. Determining a black-hole attack is a difficult work especially if the malicious node uses sequence numbers related to the ones used in the network. The black-hole attack plays a very much effect on the network

performance, which can make a network to behave like false system. The continuous increase in network overhead decreases the node's lifetime and finally leads to network destruction. Fig.5. Shows the route request and route reply in the detection of black hole node (i.e. Malicious Node) in the Network. The identification of Falsenode in the network will be discussed below in 3.2 Session.



(a) (b)

Fig.5: (a) Route Request and (b) Route Reply in the Occurrence of Black Hole Node B

3.6. Malicious Node Detection Mechanism (MNS)

The MNS Mechanism has been designed for the dynamic and scalable nature of sensor node, in which sensor nodes are replaced once they have exhausted their energy. In sensor networks, one node functioning as a monitoring node to check whether there is presence of malicious node. The monitoring node used works as follows: Immediately after Node A sends a message to Node B, it converts itself to a monitoring node, referred to here as Monitoring Node-Transmitter\Receiver (MN-TX/RX), and monitors the behavior of Node B. When Node B transmits the message to the next node, MN-TX/RX listens and compares this message with the one it has sent to Node B, thus establishing an original and an actual message. If the message transmitted by Node B is the same as the original then node MN-TX/RX ignores it and continues with its own tasks; however, if there is a difference between the original and actual messages greater than a certain threshold, the message is considered suspicious and Node B is now considered suspicious thus Node B. The Establishment of Routing Path with presence of MN-TX/RX is given in Fig.6. Each node builds a Suspicious Node table containing the reputation. Each node builds a suspicious node table containing the reputation of nodes in the cluster. Entries in this table contain the node ID, and the number of suspicious and unsuspicious entries. Nodes update this table every time they identify suspicious activity. In Table 1, ID is unique ID of sensor node: NS denotes a suspicious node and NU is the entry for unsuspicious behavior by a node. Table. 1.

Table 1: Suspicious Node

Node ID	Suspicious Entries	Unsuspicious Entries
ID	NS > 1	NU > 1

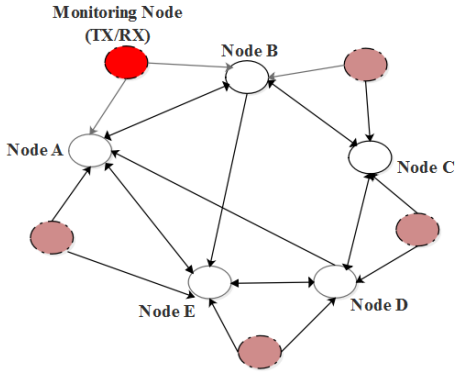


Fig. 6: Establishment of Routing Path with Presence of MN-TX/RX

The Fig.7. 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 neighbour nodes. The route establishment method is done using AODV routing protocol. If any black hole node occurs in the network then it will respond to source's request with Route Reply Packet (RREP), by obtaining that packet, the source will put the responding node to its black list. Once it is put on the black list, then knowledge based learning has been applied for confirmation of the malicious node. Almost all node get confirmation whether black hole nodes are present in the network.

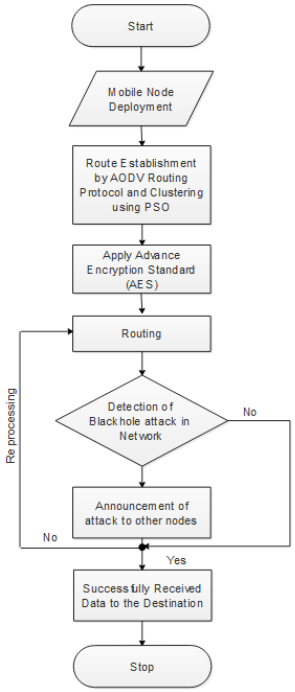


Fig.7: Flow Chart of the Overall AODV-PSO-AES-MANETs Process

4. Result and discussion

The AODV-PSO-AES method is implemented in NS2 to achieve black hole detection and obtain the optimized clustering and maintaining load balancing for data transmission using AODV-PSO algorithm. The complete work is done by using the I7 system with 8 GB RAM. The PSOalgorithm is used to obtain the optimized path and AES for secure transmission through the wireless mobile nodes.

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

i) Throughput: Throughput is calculated based on total packets received at the destination node by total network time.

ii) 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.
RH = Total no. of routing packets/Total no. of delivered data packets.

iii) Packet Delivery Ratio (PDR): Based on a total number of packets received in a ratio by a total number of destination packet sent by the source node.

iv) 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.

v) Delay/Network Latency: Different between Sending time of packets and receiving time of packets is known as delay.

vi) Packet drop/Packet loss: Total amount of packets send and packet received is known as the packet drop/packet loss.

Comparison analysis of AODV-PSO-AES is evaluated by varying the nodes 20, 40, 60, 80 and 100. The figure 8, 9, 10, 11, 12 and 13. Shows the comparison of the Through-put, Routing Overhead, Packet Delivery ratio, drop, delay and energy Consumption between existing methods.

The Comparison of Nodes vs. throughput between AODV-PSO-AES and AODV is plotted in Fig.8. The Throughput value is increased in AODV-PSO-AES method, when compared with the AODV method with different 20, 40, 60 80 and 100 Nodes.

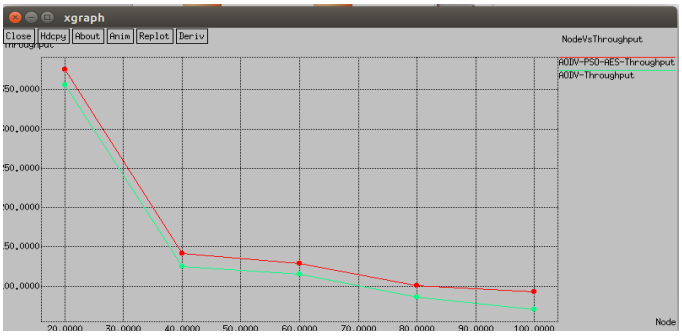


Fig.8: Nodes vs. Throughput

The Comparison of Nodes vs. Routing Overhead between AODV-PSO-AES and AODV is plotted in Fig.9. The overhead is decreased in AODV-PSO-AES method, when compared with the AODV method with different 20, 40, 60 80 and 100 Nodes.

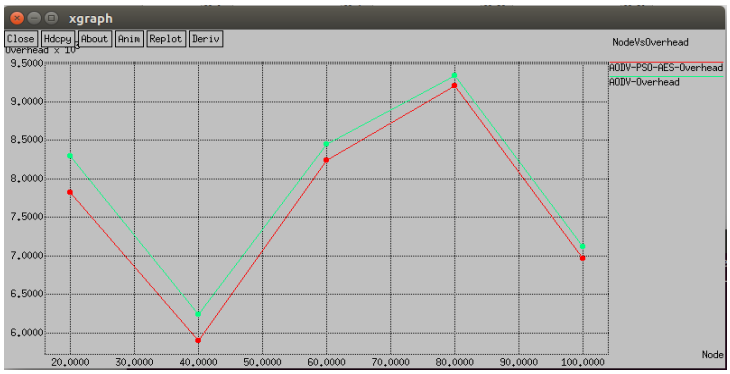


Fig.9: Nodes vs. Routing Overhead

The Comparison of Nodes vs. Delivery Ratio between AODV-PSO-AES and AODV is plotted in Fig.10. The delivery ratio is increased in AODV-PSO-AES method, when compared with the AODV method with different 20, 40, 60 80 and 100 Nodes

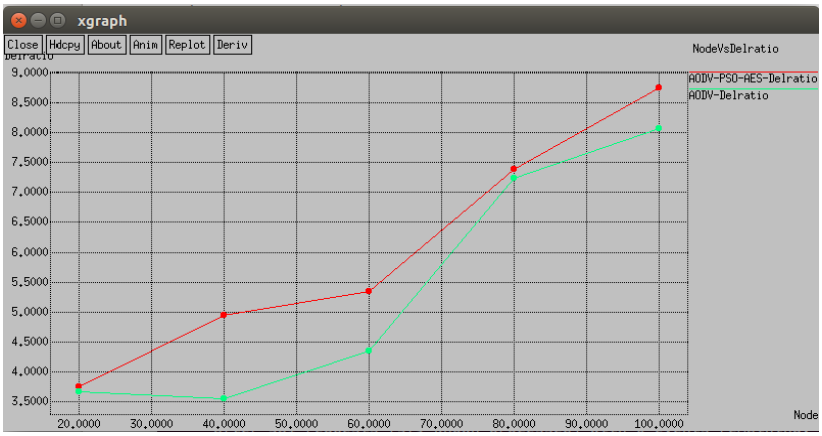


Fig.10: Nodes vs. Delivery Ratio

The Comparison of Nodes vs. Drop between AODV-PSO-AES and AODV is plotted in Fig.11. The PacketDrop is decreased in AODV-PSO-AES method, when compared with the AODV method with different 20, 40, 60 80 and 100 Nodes.

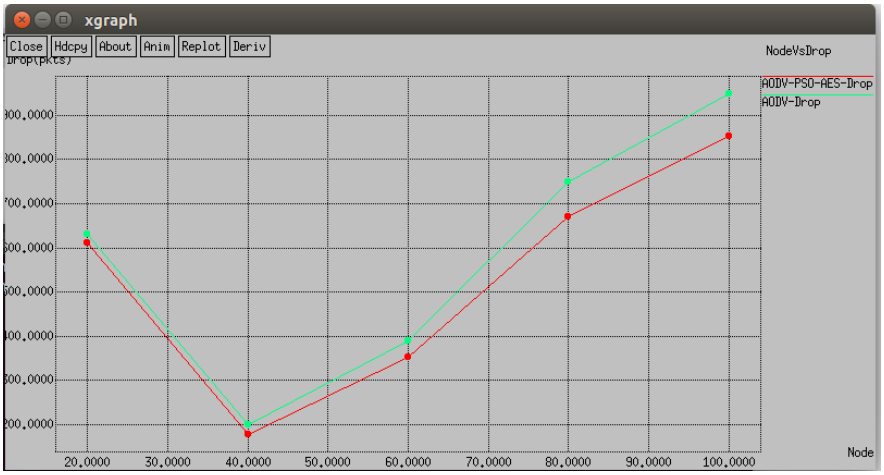


Fig.11: Node vs. Packet Drop

The Comparison of Nodes vs. Delay between AODV-PSO-AES and AODV is plotted in Fig.12. The Delay is decreased in AODV-PSO-AES method, when compared with the AODV method with different 20, 40, 60 80 and 100 Nodes.

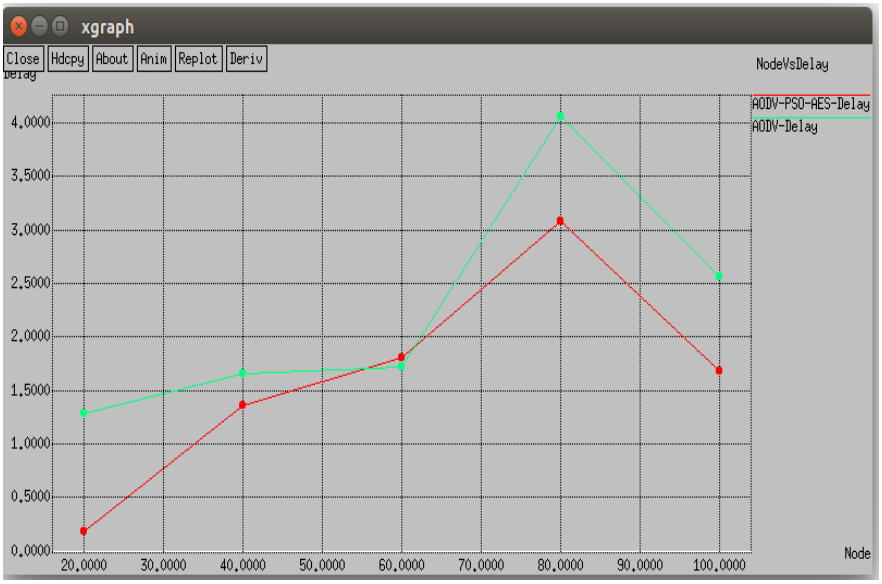


Fig.12: Node vs. Delay

The Comparison of Nodes vs. Energy between AODV-PSO-AES and AODV is plotted in Fig.13. The Energy is increased in AODV-PSO-AES method, when compared with the AODV method with different 20, 40, 60 80 and 100 Nodes.

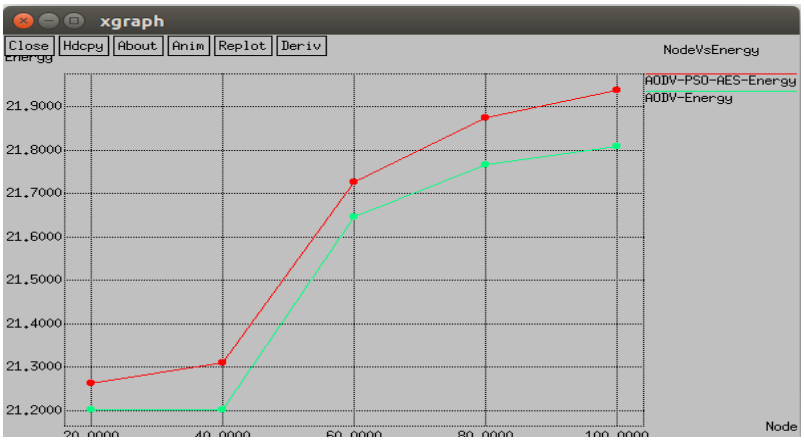


Fig.13: Nodes vs. Energy

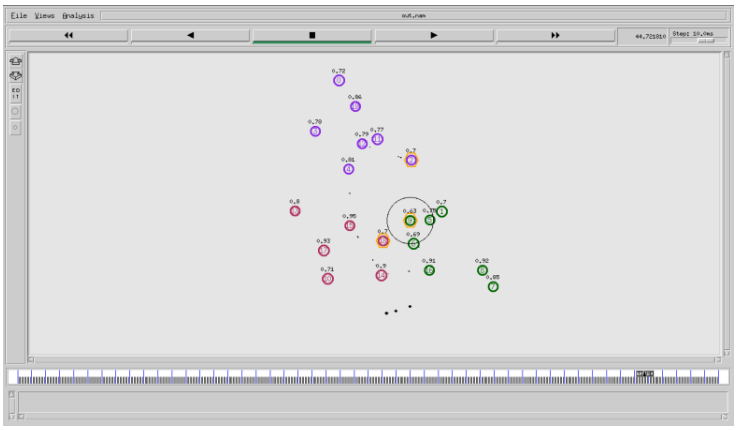


Fig.14: Data Transmission Using 20 Nodes

The Fig.14 shows data transmission takes place between 20 nodes. The Nodes 2, 9 and 18 is assigned as CH.Different color indicates different networks. The Yellow hexagonal ring indicatesCH for different networks.

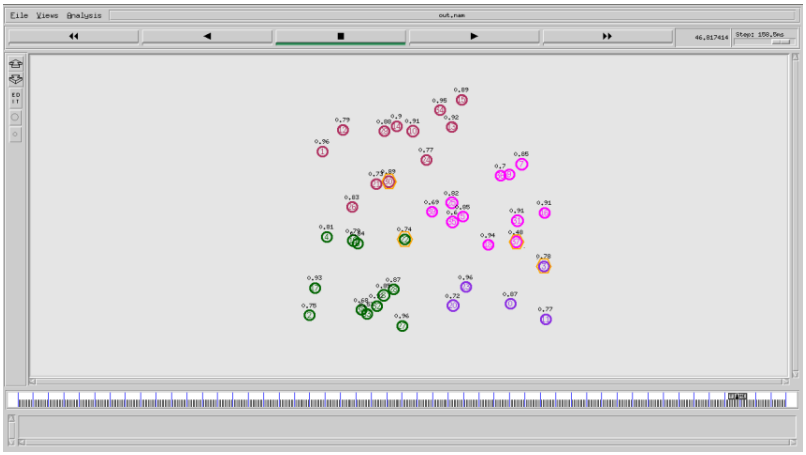


Fig.15: Data Transmission Using 40 Nodes

The Fig.15 shows data transmission takes place between 40 nodes. The Nodes 3, 22, 30 and 37 is assigned as CH. Different color in network indicates different network. The Yellow hexagonal ring indicates CH for different networks.

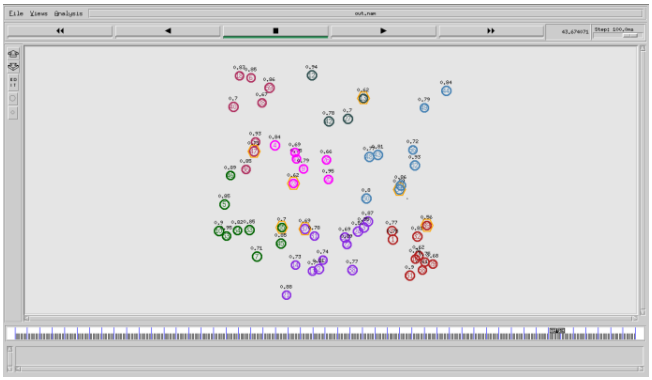


Fig.16: Data Transmission Using 60 Nodes

The Fig.16 shows data transmission takes place between 40 nodes. The Nodes 13, 23, 34, 37, 39, 47 and 55 are assigned as CH. Different color indicates different networks. The Yellow hexagonal ring indicates CH for different networks.

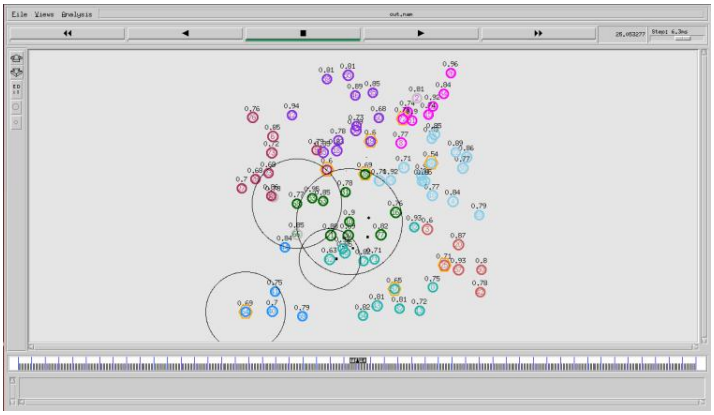


Fig. 17: Data Transmission Using 80 Nodes

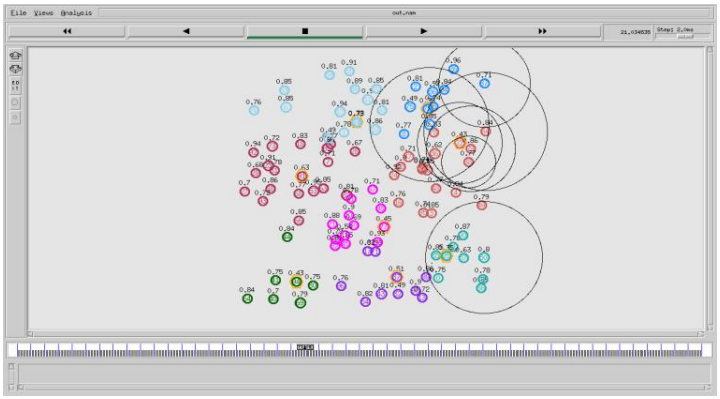


Fig.18: Data Transmission Using 100 Nodes

The Fig.17 shows data transmission takes place between 80 nodes. The Nodes 7, 19, 25, 28, 36, 37, 64 and 72 are assigned as CH.

The Fig.18 shows data transmission between 100 Nodes. The Nodes 19, 22, 25, 34, 37, 77, 79 and 91 are assigned as CH. Different color indicates different networks. The Yellow hexagonal ring indicates CH for different networks.

Specifications

Routing algorithm	AODV-PSO
Security algorithm	AES
Simulator used	NS2
Simulation start time	50.000000000
Simulation End time	146.062608572
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

5. Conclusion

In AODV-PSO-AES algorithm used todetectthe malicious attack in the network by isolating the optimized path using PSO clustering algorithm for energy consumption and maintaining load balancing. The blackhole attack is recognized using MND-TX/RX Mechanism. From obtained results, we conclude that the presented method has reached the best routing and better Through-put, Routing Overhead, Packet Delivery ratio, drop, delay and energy Consumption between existing methods for different 20, 40, 60, 80 and 100 Nodes.

References

[1] Ranjan R., Singh N.K., Singh A., Security issues of black hole attacks in MANET, International Conference on Computing, Communication & Automation (2015).

[2] Sardana A., Bedwal T., Saini A., Tayal R., Black hole attack's effect mobile ad-hoc networks (MANET), International Conference on Advances inComputer Engineering and Applications (2015), 966-970.

[3] Burbank J.L., Chimento P.F., Haberman B.K., Kasch W.T., Key challenges of military tactical networking and the elusive promise of MANET technology, IEEE Communications Magazine44(11) (2006).

[4] Jaisankar N., Saravanan R., Durai Swamy K., A novel security approach for detecting black hole attack in MANET, Information processing and management (2010), 217-223.

[5] Das R., Purkayastha B.S., Das P., Security measures for black hole attack in manet: An approach, arXiv preprint arXiv (2012).

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

[7] Su M.Y., Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems, Computer Communications34(1) (2011), 107-117.

[8] Banerjee S., Majumdar A., Saha H.N., Dey R., Modified Ant Colony Optimization (ACO) based routing protocol for MANET, In International Conference and Workshop on Computing and Communication (2015), 1-7.

[9] Singh G., Kumar N., Verma A.K., Antalg: An innovative aco based routing algorithm for Manets, Journal of Network and Computer Applications 45 (2014), 151-167.

[10] Ahmed F., Yoon S., Oh H., Bullet-proof verification (BPV) method to detect black hole attack in mobile ad hoc networks, International Conference on Ubiquitous Intelligence and Computing., Springer Berlin Heidelberg (2011).

[11] Sharma S., Singh U.K., Phuleriya K.C., Goswami D.N., SCAODV: A Protocol to Prevent Black Hole Attacks in Mobile Ad Hoc Networks.

[12] Nandini N., Aggarwal R., Prevention of black hole attack by different methods in MANET, Network 4 (2015), 297-300.

[13] Sowmya K.S., Rakesh T., Hudedagaddi D.P., Detection and prevention of blackhole attack in MANET using ACO, International Journal of Computer Science and Network Security 12(5) (2012).

[14] Patel B., Trivedi K., A review-prevention and detection of black hole attack in AODV based on MANET, International Journal of Computer Science and Information Technologies 5(3) (2014), 2816-2818.

[15] Priyanka Reddy, G.S., Surendar, A.”A review article on performance comparison of CNTFET based full adders”,(2017) Journal of Advanced Research in Dynamical and Control Systems, 9 (4), pp. 9-20.

[16] Selvi, N., Surendar, A. “Efficient power reduction and glitch free mux based digitally controlled delay line”,(2015), International Journal of Applied Engineering Research, 10 (10), pp. 9655-9659.

[17] Dhaka A., Nandal A., Dhaka R.S., Gray and black hole attack identification using control packets in MANETs, Procedia Computer Science54 (2015), 83-91.

[18] Taraka N., Emani A., Routing in Ad Hoc Networks Using Ant Colony Optimization, 5th International Conference on Intelligent Systems, Modelling and Simulation (2014).

[19] Manjusha V., Radhika N., A Performance Analysis of Black Hole Detection Mechanisms in Ad Hoc Networks, Proceedings of the International Conference on Soft Computing Systems (2016.

[20] Rajan C., Shanthi N., Misbehaving attack mitigation technique for multicast security in mobile ad hoc networks (MANET), Journal of Theoretical and Applied Information Technology 48(3) (2013), 1349–1357.