International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-11, September 2019

Secured and Efficient Data Transmission in Manets Against Malicious Attack using DSR Routing and BCS Clustering with Hybrid AES-ECC Cryptanalysis

G. Murugesan, M. Padmaa, K. Nagarajan, N. Premkumar

Abstract*: *Mobile Ad-Hoc Network (MANET) is a self-configuring network of movable nodes linked by wireless creating a random topology. The nodes are free to move randomly. Thus, the networks wireless topology may be haphazard and may alter rapidly. The efficient route is established using Dynamic source routing (DSR) Routing Protocol. The Binary crow search (BCS) algorithm is used for clustering of sensor nodes and maintaining load balancing in an efficient way. Efficient black hole detection using Malicious Node Detection Mechanism-TX/RX (MNS-TX/RX) with optimized routing algorithm is implemented in a secure environment by using Advanced Hybrid Advanced Encryption Standard (AES) cryptanalysis and Elliptic Curve Cryptosystems. Thus "DSR-BCS-HAES-EEC-MANETs" algorithm has precisely detected the black hole node and finds the proper solution for transmitting data for maintaining lifetime and Load- balancing by analyzing performance such as Through-put, routing overhead, packet delivery ratio(PDR), drop, delay and energy consumption in a secure environment.

Index Terms*: *Dynamic source routing, Mobile Ad-Hoc Network, Malicious Node Detection Mechanism, Hybrid AES and Elliptic Curve Cryptosystems.

I. INTRODUCTION

MANET is a decentralized establishment less framework wherein center points team up to propel information which is taken from a source to an objective. Where every center in a MANET exhibits patch up as a switch and amass .A couple of coordinating shows have been planned for MANETs [1] to patch up framework controlling execution. The critical issues associated with sorting not in planning appear for MANET are focus point pass on capacity, data transmission compelled and slip-up tending distant canal, asset obliged focus focuses, and active changing of the system topology [2]. MANET coordinating shows can be appointed practical or receptive guiding shows. In hands-on (table-driven) coordinating shows, each centre keeps up in any event one tables containing controlling information to one another centre in the framework. While in open (on-demand) controlling shows, courses are made awake of whatever that point to a source requires to send data to an purpose centre which infers that these shows are begun by a source on-demand. In this paper, we focus on the AODV show [3] which is one of the generally mulled over-responsive shows, considered by the IETF for systematization. Customary MANET coordinating shows expect that describe centres take an interest without threateningly exasperating the action of the show and don't give prepare for noxious aggressors. Nevertheless, the nearness of harmful centre points can't be ignored in PC frameworks, especially in MANETs in light of the remote thought of the framework. MANET procures security perils that are looked in wired similarly as remote frameworks and moreover familiarizes security strikes remarkable with itself [4] due to its characteristics. Focuses on MANET have bound tally and power confines that make the system coherently defenceless against Denial of Service (DoS) ambushes. It is hard to execute cryptography and key association figuring's which need basic estimations like open key tallies.

Center adaptability displays also an inconvenience of perceiving stale courses and fake courses. A threatening centre be able to strike the framework layer in MANET also by not sending groups or by changing a couple of the parameters of coordinating communication for instance, course of action digit and IP addresses, distribution fake messages a couple of times and transfer fake controlling information to exasperate coordinating exercises. Innumerable ambushes on MANET [5] are recognized and various game plans have been proposed to contradict them. Reenactment study have exhibited the impact of such attacks and the ampleness of proposed insurance frameworks [6] [7]. Security frameworks can be added to existing guiding shows to contradict attacks [20]. Cryptanalysis strategies are used to ensure the genuineness and uprightness of coordinating post [8]. An important concern is a tradeoff among security and execution, given the compelled resources open at various MANET centre points. Both symmetric and lopsided cryptography have been used similarly as hash mooring. Examples of these security improved shows are Authenticated Routing for Ad-hoc Networks (ARAN) [9], Secure Link State Routing Protocol (SLSP) [10], and Secure Ad-hoc On-demand Distance Vector coordinating (SAODV) [11]. Despite the authority and count cost of using cryptosystem, the display of a checked framework be more deplorable than non-confirmed inside seeing certain ambushes [12].

Manuscript published on 30 September 2019.
***Correspondence Author(s)
G.Murugesan, Assistant Professor,Department of ECE, Anjali Ammal Mahalingam College of Engineering,Tiruvarur.
Dr.M.Padmaa, Professor, Department of ECE.Saranathan College of Engineering,Trichy.
K.Nagarajan, Assistant Professor, Department of ECE,University College of Engineering, Ariyalur.
N.Premkumar, Associate Professor,Department of IT, Kongunadu College of Engineering & Technology , Thottiyam , Namakkal.

Safeguarding the channeling communication do not assurance the discovery of these hateful nodes. To conquer this problem, "DSR-BCS-HAESECC-MANETs" is implemented for increasing the performance parameters. In this work, the essential modification in DSR is used for the purpose of achieving the performance in the manifestation of black hole attack (BHA) and find efficient routing path using BCS clustering to the desired destination. The BHA is predicated using MND-TX/RX Mechanism. The HAES is used in security and it communicates with another node for the secured communication. Thus, "DSR-BCS-HAESECC-MANETs" method gives better results compared to existing method.

II. RELATED WORK

A. Aggarwal*et. al.* [12] has proposed a TSDRP protocol is evaluate result by unreliable amount of malevolent node in addition to travel connection. TSDRP assure that the envelopes are not handed over to malicious nodes and simulation result demonstrated that the PDR,is higher, end to end delay is fewer, along with throughput is maintained associated toward AODV.

S. Lee [13] has introduced the modified AODV protocol based on corroboration apply for (CREQ) and substantiation reply (CREP). If the middle knob has to drive the CREQ to its next-hop node toward the destination node in addition to RREP to the transfer node. Based ahead getting a CREQ, the next-hop node has cache for a route to the target In the event that it has a course, it sends the CREP to the source. In the wake of accepting the CREP, the source hub can affirm the legitimacy of the way by looking at the way in RREP and the one in CREP. On the off chance that both are composed, the source hub makes a decision about that the course is suitable. One disadvantage of this technique is that it can't stay away from the helpful dark hole assault if two back to back hubs cooperate as the main hub ask its next bounce hub to send CREP to the basis

Dweepnagarg*et.al.* [14] 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* [15] 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 PDR has increased but the little overhead in routing.

M. Abu Obaida*et al.* [16] presented Robust construction AODVR. AODVR has a few module for example, RREP grouping digit Tester, Blacklist Tester, Threshold Tester, extractor, Packet Classified and ALARM telecaster. In this strategy, the switch figures the scale of the received succession sums and gives the boundary esteem. On the off chance that any hub surpasses the limit esteems for a few times, it is distinguished as dark opening hub. Then again, slight system deferral is seen because of computation of the limit esteem.

DSR-BCS-HAESECC-MANETS METHODOLOGY

III. DSR-BCS-HAESECC-MANETS METHODOLOGY

The "DSR-BCS-HAESECC-MANETs" is used to identify the malicious mobile node, while network communication. The information safety is the major thing in the mobile network. Hybrid AES and ECC cryptography is used to avoid security issues in the complete network. DSR routing protocols are used for efficient route establishment, once there is a petition for a route in the network. A BHA is known as false node, which delays for others nodes to transfer Route Request (RREQ) communications. The BH attack is identified using MND-TX/RX. When the statistics is really started transmitting it absorbs all the packets and conduct to the destination. In this work, DSR-BCS-HAESECC-MANETs 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 HAESECC and BH identification using Malicious Node Detection TX/RX (MND-TX/RX).

A. Optimized self-motivated Source Routing

ODSR is a dynamic source direction-finding protocol and BCS optimization algorithm. The ODSR algorithm is simple and efficient protocol for routing which allows the multiple hop communication between mobile nodes that are not within communication range. Normally the mobile network topology changes frequently, so the routs are also change at any time. Over various jumps the ODSR permits to discover the source course to the goal by the hubs powerfully. The each arranged information bundle conveys having a header which is sent through the hubs. Therefor by incorporating the source course in the header of every datum bundle, different hubs, which are sending or catching of these information parcels can likewise reserve this steering data for some time later. There is no intermittent trade of information parcels happens in ODSR convention. The Single Route Discovery system permits of a hub to store different courses for any goal in light of the fact that the reserving of numerous courses of a hub is valuable to discover another course on the off chance that one course fall flat. The ODSR protocol is based on three mechanism that effort together to permit the innovation optimization and preservation of source routes.

B. Optimization using BCS

ODSR algorithm helps for create the multiple routes among the transmitter and receiver. The major objective of this work is to improve the route in the MANET with the help of BCS. The BCS helps to select the optimal route depends on average delay. Population of multiple paths discovered is by BCS. Fitness value of each particle is evaluated based on average delay. The detailed description of the optimization is described in [18].

C. Route Maintenance

Due to the topology change source mobile node can't make the route but which can able to identify the data envelop.

Whenever the neighboring node is disconnected at the time an error message RERR will generate and which transferred to route transmitter node. After receiving RERR the source node disconnect all the links and start the new route prediction.

D. Hybrid AES-ECC

AES and ECC are the two most regularly utilized symmetric and hilter kilter encryption calculations. In this work, AES and ECC algorithm are combined, which can solve the problem such as password system speed and security, which can't proficiently understand the data, information encryption, mark and personality check. What's more, the cross breed encryption is connected into the email framework to improve the system security of data transmission. Hybrid AES-ECC Encryption and Decryption Frameworks are shown in figure.1. And figure.2.

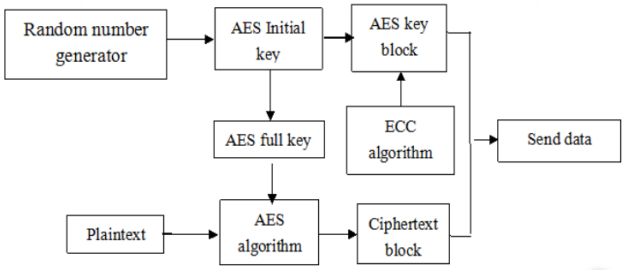

Figure.1.Hybrid AES-ECC Encryption Framework.

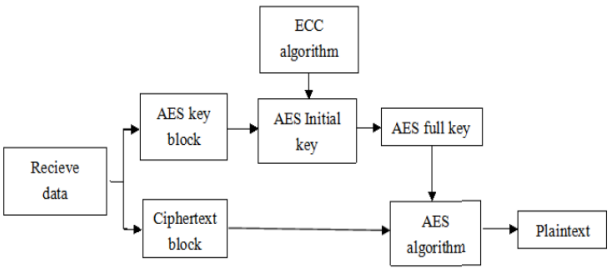

Figure.2.Hybrid AES-ECC Decryption Framework.

E. BHA Detection

The false node responds to routing request from side to side a large sequence amount, least hop. The source node transmits data to the receiver over the BH mobile node. By this way, a BH mobile node diverts most of a traffic of the network to itself and it drops the data. Determining a BHA is a challenging work particularly if the malicious node uses sequence amounts related to the ones used in the system. The dark opening assault plays a particularly impact on the system execution, which can make a system to carry on like false framework. The stable increment in system overhead abatements the hub's lifetime lastly prompts organize decimation. Figure.3. Shows the route request and route reply in the detection of black hole node in the System. The identification of False node in the system will be discussed below in 3.2 Session.

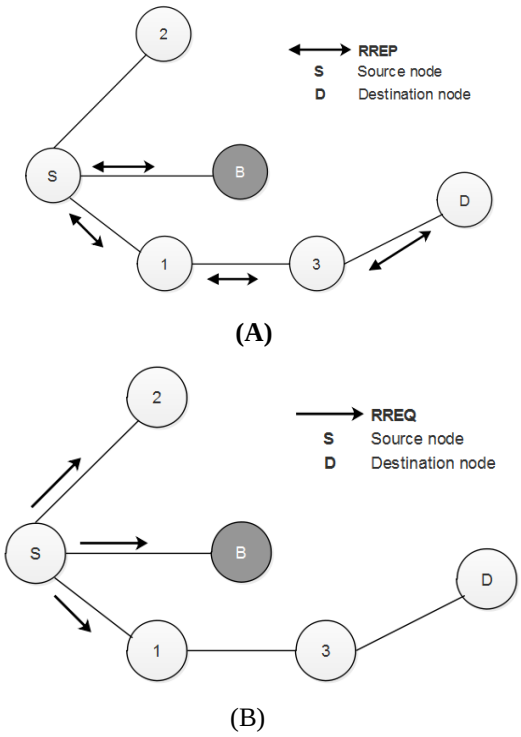

Figure.3. (a) Route request and (b) Route reply in the occurrence of black hole node B

F. Malicious Node Detection Mechanism (MNS)

The MNS device have been intended for the lively and versatile natural world of sensor hub, in which sensor hubs are supplanted once they had depleted their vitality [20]. In sensor networks, one node functioning as a monitoring node to check whether there is presence of malicious node. The checking hub utilized functions as pursues: Immediately after Node A makes and impression on Node B, it changes over itself to an observing hub, alluded to here as Monitoring Node-Transmitter\Receiver (MN-TX/RX), and screens the conduct of Node B. When Node B transmits the message to the next node, MN-TX/RX listen and compare this communication with the one it has sent to Node B, thus establish an original and an real message. On the off chance that the point transmit by Node B is equivalent to the first then hub MN-TX/RX overlooks it and proceeds with its own errands; in any case, if there is a contrast among the first and genuine communication more prominent than that of a specific limit, the message is viewed as doubtful and Node B is currently viewed since mistrustful consequently Node B.The Establishment of Routing Path with presence of MN-TX/RX is given in Figure.4.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

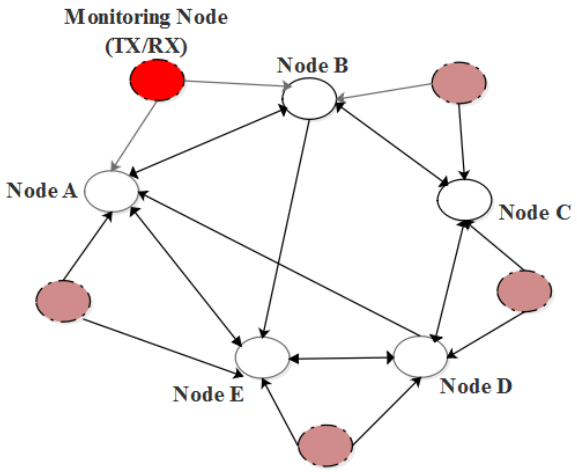

Figure. 4. Establishment of Routing Path with Presence of MN-TX/RX

The figure.5. Defines the flow routing process. Here a finite amount of mobile nodes is organized in the specified area and originally, transmitter and receiver are allocated. Formerly transmitter and receiver are well-defined then transmitter mobile node transmission an RREQ to all the neighbor mobile nodes. The route establishment method is done using AODV routing protocol. If any black hole node occurs in the system then it will respond to transmitter demand with Route Reply Packet (RREP), by gaining that envelope, the transmitter will put the answering to the mobile node as black list. Once it is put on the black list, then knowledge established learning has been applied for validation of the malicious node. Almost all node get confirmation whether black hole mobile nodes are contemporary in the network.

IV. RESULT AND DISCUSSION

The DSR-BCS-HAES-EEC-MANETs method was implemented in Matlab 2018 to detect the black hole detection and obtain the optimized clustering and maintaining load balancing for data communication using DSR-BC S system. The entire work is completed with the help of I3 computer with 2 GB RAM. The BCS calculation is utilized to acquire the improved way and HAES-EEC for the secure transmission through the versatile hubs. That area gives a point by point perspective on the outcomes that are gotten utilize DSR-BCS and HAES-EEC framework. DSR-BCS-HAES-EEC-MANETs calculation is utilized for giving security to the messages controlled in the hubs.

The trial consequences and the presentation of Through-put, PDR, routing overhead, compartment drop, postponement and vitality are compared with existing method. The presentation is planned by measuring in the terms of throughput, routing overhead, PDR, parameters Throughput and PDR. The Presentation metrics is defined below;

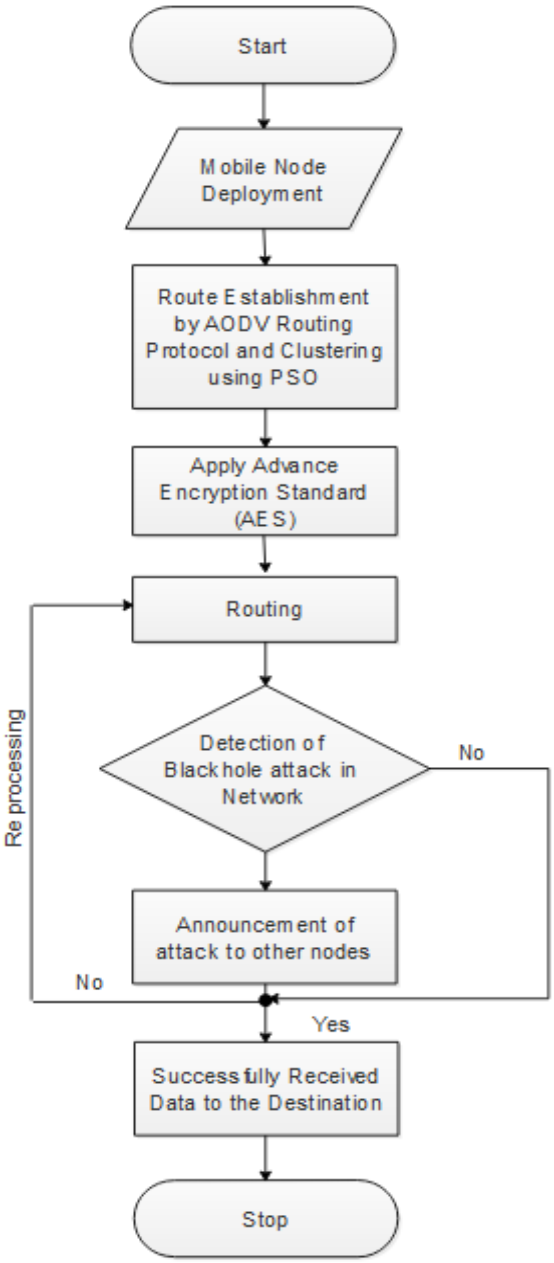

Figure.5. Flow chart of the overall AODV-PSO-AES-MANETs Process.

A. Throughput

Total amount of envelopes received at the beneficiary mobile node by whole network time.

B. Routing Overhead

The quantity of direction-finding envelopes requires for network communication, which is separated by a total amount of received facts packages.

RH = Overall no. of routing envelopes/Overall no. of delivered data envelopes.

C. PDR:

A total amount of envelopes received in a ratio by a nover all amount of goal envelope transferred by the source node.

Retrieval Number: J94840881019/19©BEIESP
DOI: 10.35940/ijitee.J9484.0981119
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

D. Energy consumption:

The enormous number of bounces is comparable to the tremendous measure of got vitality utilization. A hub drop a specific measure of vitality for each parcel broadcast and accepting.

E. Delay

Different among the envelope transmitting time and envelope receiving time is named as delay.

E. Packet drop

Total quantity of envelopes send and envelope received is known as the packet or envelop drop ratio.

Comparison analysis of DSR-BCS-HAES-EEC-MANETsis evaluated by varying the nodes such us 20, 40, 60, 80 and 100. The Comparison of Nodes vs. throughput between DSR-BCS-HAES-EEC-MANETs and AODV-PSO-AES is defined in figure.6. The Throughput value is improved in DSR-BCS-HAES-EEC-MANETs method, when compared with the AODV-PSO-AES method.

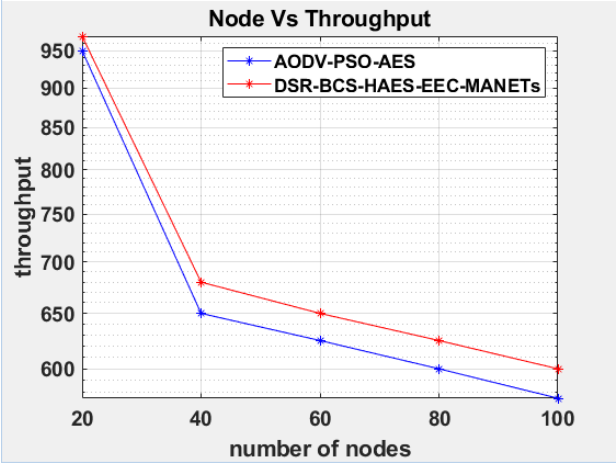

Figure.6. Comparison of Mobile nodes and throughput.

The Comparison of mobile nodes and Routing Overhead between DSR-BCS-HAES-EEC-MANETs and AODV-PSO-AES isdefined in figure.7. The overhead is reduced in DSR-BCS-HAES-EEC-MANETs method, when compared with the AODV-PSO-AES method.

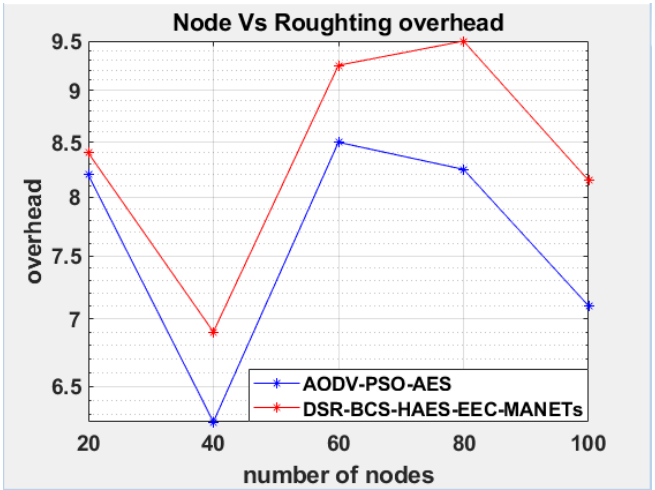

Figure.7.Comparison of Nodes vs. Routing Overhead.

The Comparison of Nodes vs. Delivery Ratio (DR) between DSR-BCS-HAES-EEC-MANETs and AODV-PSO-AES is defined in figure.8.

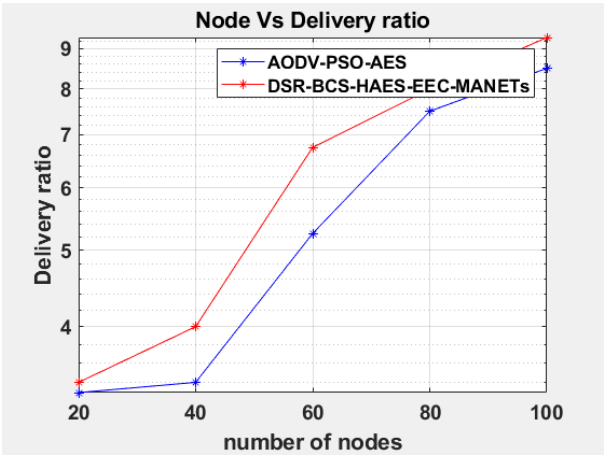

Figure.8.Comparison of Nodes vs. DR.

The Comparison between Nodes vs. Drop between DSR-BCS-HAES-EEC-MANETs and AODV-PSO-AES isshowed in figure.8. The Packet Drop is reduced in DSR-BCS-HAES-EEC-MANETs method, when compared with the AODV-PSO-AES method with various mobile nodes structure.

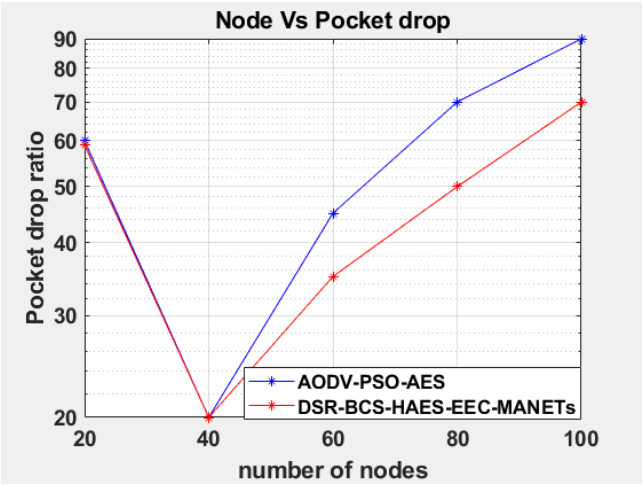

Figure.8.Comparison of Nodes and Pocket drop Ratio.

The Comparison of Nodes vs. DR between DSR-BCS-HAES-EEC-MANETs and AODV-PSO-AES is shows in figure.11. The DR is increased in DSR-BCS-HAES-EEC-MANETs method, when compared with the AODV-PSO-AES method with variousmobile Nodes**.**

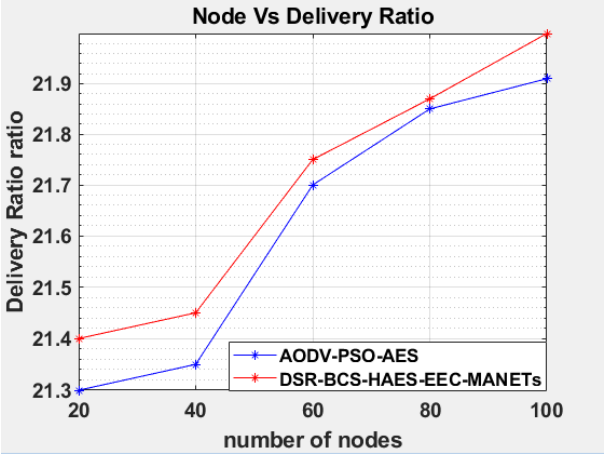

Figure.9. Comparison of Nodes vs. DR.

V. CONCLUSION

In DSR-BCS-HAES-EEC-MANETs algorithm used to detect the malicious attack in the MANET by isolating the improved path using BCS clustering algorithm for energy consumption and maintaining load balancing. The blackhole attack is recognized using MND-TX/RX Mechanism. From achieved results, we conclude that the DSR-BCS-HAES-EEC-MANETs method has provide the better routing results. And also the proposed system provides better Routing Overhead, PDR, Through-put, energy Consumption and pocket delay compared to other existing systems.

REFERENCES

1. A. Boukerche, B. Turgut, N. Aydin, M. Ahmad, L. Bol¨ oni, and ¨ D. Turgut. Routing protocols in ad hoc networks: a survey. Computer Networks, 55(13):3032–3080, September 2011.
2. M. A. Abdelshafy and P. J. King. Analysis of security attacks on AODV routing. In 8th International Conference for Internet Technology and Secured Transactions (ICITST), pages 290–295, London, UK, Dec 2013.
3. C. E. Perkins and E. M. Royer. Ad-hoc on-demand distance vector routing. In Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, pages 90–100, 1997.
4. A. Kumar. Security attacks in MANET - a review. IJCA Proceedings on National Workshop-Cum-Conference on Recent Trends in Mathematics and Computing 2011, RTMC (11), May 2012.
5. M. Singh, A. Singh, R. Tanwar, and R. Chauhan. Security attacks in mobile adhoc networks. IJCA Proceedings on National Workshop-CumConference on Recent Trends in Mathematics and Computing 2011, RTMC (11), May 2012.
6. R. Kiruba Buri and T. Jayasankar, "Intelligence Intrusion Detection Using PSO with Decision Tree Algorithm for Adhoc Networks", Bioscience Biotechnology Research Communications, Special Issue Recent Trends in Computing and Communication Technology, Vol. 12, No.2, March (2019),pp.27-34
7. G. Usha sand S. Bose. Impact of gray hole attack on adhoc networks. In International Conference on Information Communication and Embedded Systems (ICICES), pages 404–409, 2013.
8. P. Joshi. Security issues in routing protocols in MANETs at network layer. Procedia Computer Science, 3:954–960, 2011.
9. K. Sanzgiri and et al. Authenticated routing for ad hoc networks. IEEE Journal On Selected Areas In Communications, 23:598–610, 2005.
10. P. Papadimitratos and Z. J. Haas. Secure link state routing for mobile ad hoc networks. In Symposium on Applications and the Internet Workshops, pages 379–383. IEEE Computer Society, 2003.
11. M. G. Zapata. Secure ad hoc on-demand distance vector routing. SIGMOBILE Mob. Comput. Commun. Rev., 6(3):106–107, jun 2002.
12. M. A. Abdelshafy and P. J. King. AODV & SAODV under attack:performance comparison. In ADHOC-NOW 2014, LNCS 8487, pages 318–331, Benidorm, Spain, Jun 2014.
13. S. Lee, B. Han, and M. Shin. Robust routing in wireless ad hoc networks. In International Conference on Parallel Processing Workshops, pages 73–78, 2002.
14. Garg, Dweepna, and ParthGohil. "Ant Colony Optimized Routing for Mobile Ad Hoc Networks (MANET)." International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN) 2.3, 4 (2012).
15. Dhaka, Arvind, AmitaNandal, and Raghuveer S. Dhaka. "Gray and Black Hole Attack Identification Using Control Packets in MANETs." Procedia Computer Science 54 (2015): 83-91.
16. M. Abu Obaida, S. A. Faisal et al., "AODV robust (AODVR): Ananalytic approach to shield ad-hoc networks from black holes",International Journal of Advanced Computer Sciences andApplications, vol. 2, issue 8, pp. 97-102, 2011.
17. H.Weerasinghe and H. Fu. "Preventing Cooperative black holeattacks in mobile adhoc networks:simulation implementation andevaluation", Future generation communication and networking,volume 2,IEEE 2007, pp. 362-367.
18. A. Aggarwal, S. Gandhi, N. Chaubeyet. al. "Trust Based Secureon Demand Routing Protocol (TSDRP) for MANETs", IEEEProceedings of International Conference ACCT, 8-9 February,2014, DOI 10.1109/ACCT.2014.95
19. R.ArunPrakash, K.VinothKumar, T.Jayasankar, "Detection, Prevention and Mitigation of Wormhole Attack in Wireless Ad Hoc Network by Coordinator", Appl. Math. Inf. Sci. vol.12,no.1, Jan 2018, pp.233–237.
20. E.Vishnupriya, T. Jayasankar and P. Maheswara Venkatesh, " SDAOR: Secure Data Transmission of Optimum Routing Protocol in Wireless Sensor Networks For Surveillance Applications, ARPN Journal of Engineering and Applied Sciences, Vol. 10,Issue. 16, Sep 2015,pp 6917-6931.