International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-4S5, December 2019

A Biogeography-Based Optimization (BBO) With AOMDV for Mitigating Black Hole Attacks

G. Mahalakshmi, A. Suresh

Abstract*: The availability of smaller, cheaper and a lot more powerful mobile devices has made the Mobile Ad Hoc Networks (MANETs) emerge as a fast-growing research area. A Black Hole Attack can harm the mobile nodes by giving false replies to its source which can have the path that is the shortest to the destination without it checking the routing table. The primary aspect relaying the strategy of the trust route was the generation of a route by the selection of nodes that have high trust; thus, the nodes having the maximum trust measure with a better probability of routing success. One of the recently proposed metaheuristic that is applied successfully to various problems of optimization owing to its efficiency and simplicity is the Biogeography-based optimization (BBO). The BBO generally performs well for the problems of low-dimensional optimization but the performance keeps deteriorating rapidly for high-dimensional problems. In this work, proposed a BBO – Ad-hoc on Demand Multipath Distance Vector (AOMDV) method to mitigate black hole attack.

Keywords* : Black Hole Attack, Biogeography-based Optimization (BBO) and BBO – AOMDV method, Mobile Ad Hoc Networks (MANETs) and trust.

I. INTRODUCTION

Mobile Ad hoc Networks (MANETs) has been defined as the wireless network consisting of mobile nodes that communicate with one another in a fashion which is multi-hop without the support of the fixed infrastructure like the base stations, access points or wireless gateways. Owing to this, the MANETs were known as the infrastructure-less or the non-infrastructure wireless networks. Ad hoc refers to the network that is established for a particular reason, generally extemporaneous services are customized to certain specific applications. The MANETs can enable the environments of wireless networking in the absence of cellular or wired infrastructure or something that is not sufficient in terms of cost. Not having base stations or central coordinators can make the MANETs complex in various types of wireless networks like the wireless local area networks (WiFi). The issues to security in the MANET communications can be demanding [1] owing to the involvement of several paths from the source to its destination.

Finding multiple routes between the sender and the receiver is called Multipath routing. These paths can be node disjointed or overlapped with one another. The AOMDV is a multipath routing protocol used to compute link disjoint and loop-free paths. The AOMDV attempts at finding more routes between the source and the destination where the path is dis-joined. An alternate route can be used when one route fails. The AOMDV has a lesser number of paths and the main advantage of it is the reduction of overheads and reduced delay [2].

The AOMDV Routing Protocol has been one of the most commonly used protocols of Ad hoc routing. This is reactive in nature and is DSDV-based. It is a multipath protocol and is a combination of the destination sequence number found in the DSDV and the technique of route discovery of a DSR protocol. It computes multiple paths that are loop-free in the process of route discovery. The availability of such multiple paths, make the protocol to switch from one such route to the next one that is the best at the time the earlier route fails. This new process of route discovery has been initiated only at the time the paths to one particular destination fails. These loop-free link disjoint paths with multiple routing can be quite effective as it can bring down routing overheads and better support load balancing. It can also avoid congestion as routes as alternate routes are available. These multiple paths have been formed through neighbors by which the RREQ and the RREP are obtained. The selection of an alternate route in case of routing failure can eliminate the latency of route discovery [3].

MANET security can provide anonymity, authenticity, authorization, integrity, confidentiality, and availability. For the transmission of secure information, the security of MANET communication is crucial. The absence of a mechanism of central co-ordination with a shared wireless medium can make the MANET vulnerable to cyber-attacks. The degree of belief regarding the behavior of other entities is known as trust. The nodes that take part in exchange of data have to be shielded by trust along with mechanisms of reputation and if not they may be attacked resulting in unwanted consumption of resources. These attacks may either be direct or indirect as intruders can take complete charge of the good nodes that result in issues of non-cooperation thus resulting in the destruction of the network.

Thus, there is a need to identify nodes that are prone to compromise through the reputation and trust mechanisms to make sure the network is safe. The trust agent gets trust levels from the events that are experienced by the node.

Revised Manuscript Received on December 5, 2019.

G. Mahalakshmi*, Guest Lecturer, Computer Science, Muthurangam Govt. Arts College (Autonomous), Otteri, Vellore - 632 002, priyamahamga@gmail.com

Dr. A. Suresh: M.C.A., M.Phil., Ph.D., SET. Principal, Computer Science, SIRI PSG College of Arts and Science for Women, Sankagiri.asuresh1975@yahoo.com

A classical issue found in various areas bound with the day-to-day lives of people is optimization. Recently, the development of human civilization and the industry has raised several complicated issues.

At the same time, there are several corresponding approaches that are being proposed to solve them. One of such approaches is metaheuristics inspired by the natural phenomena of various types of algorithms. These meta-heuristic algorithms are superior in dealing with problems of optimization and combinatorial optimization.

Evolutionary algorithms (EAs) have been found to be very efficient in solving complex problems in optimization. Biogeography-based optimization (BBO), that was proposed in the year 2008 by Simon has been inspired by biogeography of migration of species between various habitats, their evolution, and extinction. By assuming the problem every habitat will represent a new candidate solution and the features of the habitat will represent the decision variables. Based on the biogeography theory, any solution that is superior will share promising information with a one that is inferior by migration that includes high emigration and low immigration and vice versa. Mutation can take place with a particular probability based on the evolution of biogeography.

In this paper we proposed Biogeography-based optimization with AOMDV protocol to improve the network performance. Section 2 reviews the literature for the related works of trust based routing in MANET. Section 3 explains the methodology and section 4 discusses the experimental results. Section 5 concludes the proposed work.

II. LITERATURE SURVEY

The MANET, with its dynamic nature, can degrade the reliability of the transmission of data. It is not protected against attacks owing to the lack of security. One of the most common attacks experienced in the MANET is the black hole attack. Selvavinayaki and Karthikeyan [4] had addresses certain solutions that were security-oriented in order to prevent black hole attacks with digital certificates that could authenticate routes at the time of route discovery. The authentication of digital certificates can avoid black hole nodes during route discovery. This is implemented based on the and is simulated with the NS2.

Another major challenge in the MANET can be the Black Hole Attack which is against the integrity of the network that absorbs all the data packets. As these data packets do not manage to reach the destination node owing to this attack loss of data will take place. The Black Hole Attack can harm the mobile nodes by means of falsely replying to their source node which will be the shortest path to their destination without any check on the routing table. Thus, the source node can send all data to this black hole node and swallows the packets sent from the source node. Pandikumar et al [5] had further applied a new measurable technique to mitigate black-hone nodes. The method applied an Intrusion Detection System (IDS) that was based on an anomaly to protect availability, integrity, and confidentiality. The method was also verified by means of running the simulations by NS2 that were either with or without a black hole attack through the AOMDV (Ad hoc on Demand Multipath Distance Vector) protocol. The performance metrics showed that the IDS could achieve remarkable results of the packet delivery ratio which was up to 99.75%.

Security is a critical concern in the MANET system that is vulnerable to attacks in the Mobile Ad-Hoc Networks (MANETs. To design a good protocol for security of the MANET can be challenging owing to its unique traits. They are physical vulnerability, resource availability, lack of user association, an insecure environment of operating, and shared radio channels. Bansal and Gupta [6] had brought about a study based on simulation of the impact on the attack of neighbors and the black hole attack on the routing protocol of the AOMDV by means of calculating metrics of performance like throughput, end-to-end ratio, and packet delivery ratio. The wireless links can make the MANETS prone to attacks and this study has proposed a trust mechanism for mitigating the wormhole attack in the MANETs. There are several techniques of optimization to identify the optimal path from a source to the destination. Dorai and Rajaram [7] had extended trust and reputation for improving the quality of the link along with an Ad hoc On-demand Multipath Distance Vector (AOMDV) based on channel utilization. Differential Evolution (DE) was employed for optimization.

The problems in security and efficiency of energy have been considered to be the supreme factors in the MANETs and the threats to security emerged owing to their scares traits of resources. Thus, all their functionalities were degraded with several attacks on security and the cruel Black Hole Attack (BHA). This primarily distresses the collection of data and attempts at engaging in the links for increasing the issues that are resource-constrained. For withstanding such issues Merlin and Ravi [8] had proposed another novel Trust-based Energy-Aware Routing. The most important traits of the TEAR were that it can mitigate the BHs by means of a dynamic multiple detection route generation. This was to detect the BHs fast and provide better security by means of nodal trust. This mechanism was able to handle creation, as well as the sharing of multi-detection routes for detecting the BHs. These multi-detection routes in the mechanism were generated by using the energy in certain non-hotspots (without wastage of energy) for improving the efficiency of energy and route security. An analysis, both theoretical and experimental was made to prove the TEAR mechanism exhibited performance that was better compared to earlier research. This could optimize the network lifespan by means of avoiding black hole attacks and improving routing.

Guo et al [9] had proposed a survey for this in which firstly the basic BBO operators were introduced that included migration and mutation.

The former mimics the migration of species among the islands and this provided a way of recombination for the candidate solutions for interacting with one another to improve the entire population. Aside from the linear model for migration, there were other popular models that had been introduced and their performance was analyzed. For a mutation operator, the BBO design is found different. In a standard BBO, there are different rates of migration for different candidate solutions and their rate of the assignment will influence the performance. Secondly, certain popular BBO variants were summarized and the related hybrid algorithms had enhanced performance. This further introduced a development to the algorithm helping readers understand how to select the right type of BBO for any problem. This helps the performance of the algorithm and also in designing newer variants for certain specific issues. Thirdly, there was a performance evaluation made for the BBO and the results proved that the BBO was competent in solving problems of optimization. In spite of several of these achievements of the BBO, there are many open issues that have to been solved in the future in order to render this algorithm even more competitive in the field of metaheuristics.

Biogeography-based optimization (BBO) can be called an evolutionary algorithm that is inspired by the habitats and migration of species. It has been more than 10 years since the first paper on BBO was published in the year 2008. It has been able to solve problems in optimization successfully in various domains and has reached a mature state. Taking the significant expansion of research into consideration, it can be said that this is the right time to make a 10-year anniversary review with published literature. Maet al [10] had summarized and further organized the literature for the last 10 years of BBO research. This begins with the foundation of a basic BBO and the family of these algorithms is reviewed and discussed to make applications, hybridizations, and modifications in engineering and science. Lastly, the paper also proposed some open and interesting issues aside from showing future research directions for the BBO.

III. METHODOLOGY

This section details on Black Hole Attack, Adhoc On-demand Multipath Distance Vector (AOMDV) and Proposed Biogeography-Based Optimization (BBO) - Adhoc On-demand Multipath Distance Vector (AOMDV).

A. Black Hole Attack

In Black Hole attack, malicious nodes will wait for neighbors to initiate the RREQ packet. When the nodes get the RREQ packets, it sends a false RREP packet that has a modified sequence number that is higher. Now the source node will assume the node to have a fresh route to the destination [4]. It ignores the RREP packet from the other nodes and sends data packets via the malicious nodes which in turn does not permit packet forwarding. This is called the black hole attack as the data packets and objects are all dropped.

B. Adhoc On-demand Multipath Distance Vector (AOMDV)

Based on the ideal of the distance vector and on the usage of hop-to-hop routing, the AOMDV can discover on-demand routes with a unique technique for discovery. The main difference between that of the AOMDV and the AODV is found in route discovery [11]. The very essence of this AOMDV protocol rests on the fact that multiple paths are guaranteed and are both disjoint and loop-free. To find these routes making use of a flood-based discovery the route updates will run in the AOMDV and are locally executed for every node having a major role in the maintenance of disjoint attributes and loop freedom.

The AOMDV further extends the AODV to discover multiple paths that exist between the sender and the receiver. Route entries for all destinations will consist of a small list of hops with compatible hop counts. The sequence number for the whole hop will be the same and is useful in keeping track of the route. The node further maintains the advertise of hop count for all such destinations. For the paths defining a maximum hop count used for forwarding route advertisement to the destination, another alternate path will be assured loop freedom for the node. In case it has a lower number of hop counts compared to the advertised one, the alternate method is followed. For one sequence number, there is no change in the hop count. The subsequent hop list and their advertised hop counts will be reinitiated at the time the route advertisement has a higher sequence number [12].

The AOMDV protocol uses an intermediate node and the RREQ has some duplicate copies that do not get discarded. The RREQs will have to come from different neighbors and the RREQ packet will be verified using the first hop field along with the first hop list that is used for the RREQ packet. In the destination level, another approach will be employed where the path gets decided for a link-disjoint. From the same destination, the replies come from n copies of an RREQ irrespective of the first hop. The AOMDV normally works in two different phases: 1) For every node, there is a rule of route update for maintenance and establishment of many loop-free paths. 2) The link disjoint paths will be found using a distributed protocol. The advantages of the AOMDV are [13]: a loop-free node that is created by the AOMDV can maintain connectivity, is fast and efficient in recovery and is an established on-demand route.

The Route Discovery Process: At the time source node S intends to find a route to its destination node D, it will attempt at identifying whether the Routing table has a readily available route. In case there is no route available, the route will broadcast the RREQ packet to its neighboring nodes.

At the time of arrival of the RREQ packet, the RREQ will be scanned. In case the destination address for the RREQ is similar to that of the intermediate node, it will act as the destination node and forward a route reply. If not it will rebroadcast the RREQ.

Either the destination node or any other node with a valid route to its destination will reply. The RREP packets found in a security-enhanced AOMDV will be similar to that of the DSR. A malicious node can reply to the request from a source that is done by claiming to have a path that is the shortest to its destination. All disjoint routes will be stored in the routing table. A K-level shortest path algorithm will be employed for identifying the shortest path for the disjoint links. All stored routes found in a routing table will be sorted based on the cost of communication.

C. Proposed Biogeography-Based Optimization (BBO) - Adhoc On-demand Multipath Distance Vector (AOMDV).

Biogeography-based optimization (BBO) had been introduced in the year 2008 for solving problems of global optimization [13]. This was an evolutionary algorithm motivated by the habitats and migration of species. The BBO demonstrated to be very powerful and included strategies of exploration and exploitation. It is a nature-inspired algorithm that is suitable to solve practical problems of optimization. It is computationally efficient, flexible and simple and is also stochastic in nature, not needing derivatives of an objective function.

By means of abstracting a species migration mechanism in different islands, these Biogeography-based optimization methods mimic the distribution of the species in natural biogeography. The island in the BBO [14] is not only a small piece of land surrounded by water but an area that is isolated geographically. In biogeography, the quality of geographical areas can be judged by taking various elements into consideration that include humidity, temperature, and climate. All these elements are known as the Suitability Index Variables (SIVs), and the actual quality of the island the Habitat Suitability Index (HSI). In those areas suitable for species to live, there has to be a large HIS value. So, the capacity of good areas is quite saturated and it is challenging to immigrate to such areas but very easy to emigrate from them. Also for the poor areas, it is easy to immigrate but challenging to emigrate. In the BBO, a poor solution will be analogous to the area with a low HIS and a good solution means the area has high HIS. Based on the BBO mechanism, the solutions that are good will have a high chance of sharing the SIVs to other solutions and low chances of accepting SIVs. At the same time, poor solutions have higher probabilities of accepting SIVs from other solutions. This can be quite similar to the migration of species among good or poor areas.

Fig 1 shows the flowchart for Proposed Biogeography-Based Optimization –AOMDV.

Proposed BBO – AOMDV Algorithm:

(1) Initializing of the parameters of the BBI (including getting a scheme of representation for the habitats dependent on problems and initializing the rate of maximum migration, rate of maximum mutation and the elitism parameter).

(2) Initializing a set of habitats that correspond to potential solutions. Implementation of the AOMDV routing Protocol.

(3) Associate habitats with the rate of immigration and emigration based on HSI.

(4) Perform migration probabilistically for modifying every one-elite habitat. Now, re-compute every HSI.

(5) Associate every habitat with the rate of mutation according to its species count.

(6) Perform mutation probabilistically for modifying every non-elite habitat. Not re-compute every HSI.

(7) Now g to step (3) for the subsequent iteration and repeat until such time a predefined number of generations are met or this is done after a certain acceptable solution is found.

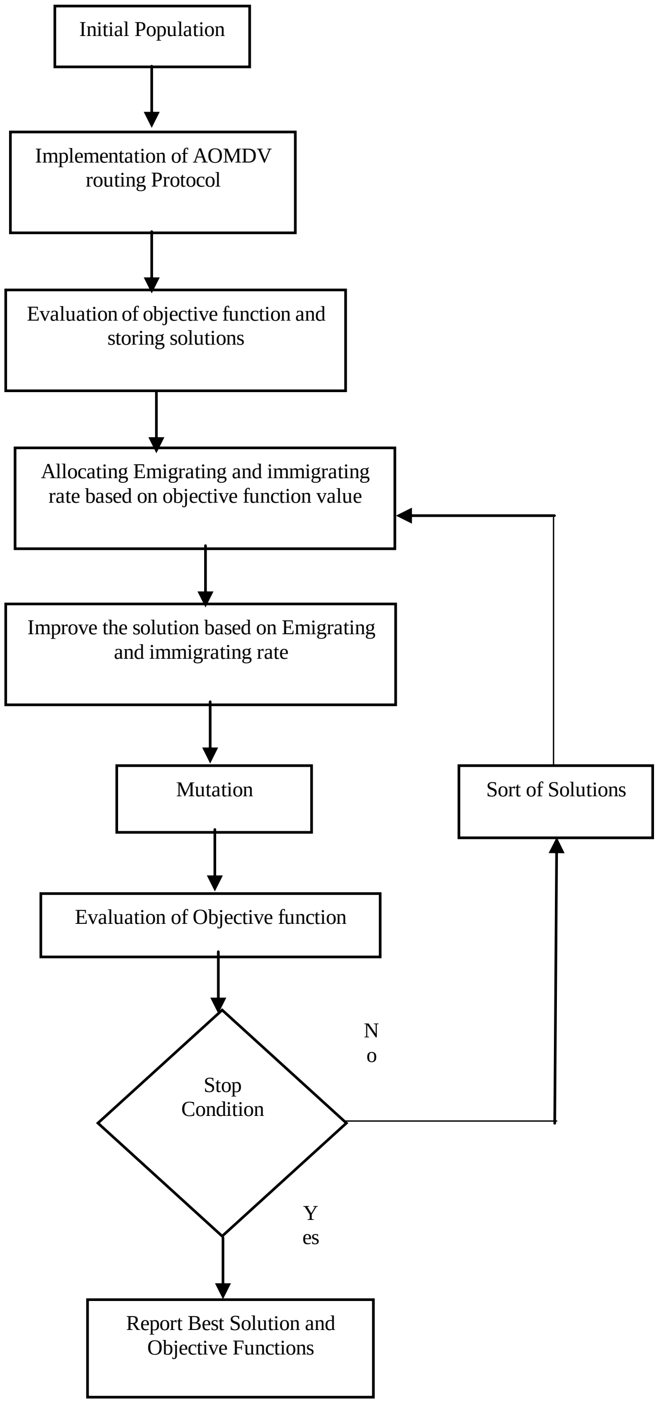
Initial Population
Implementation of AOMDV routing Protocol
Evaluation of objective function and storing solutions
Allocating Emigrating and immigrating rate based on objective function value
Improve the solution based on Emigrating and immigrating rate
Mutation
Sort of Solutions
Evaluation of Objective function
Stop Condition
No
Yes
Report Best Solution and Objective Functions

Fig1 Flowchart for Proposed Biogeography-Based Optimization –AOMDV

IV. RESULTS AND DISCUSSION

Experiments conducted to calculate packet delivery ratio, end to end delay, number of hops to destination and percentage of malicious nodes detected. The results listed in Tables I to IV and Figure 2 to 5 shows the Trust-5% Malicious, Trust-10% Malicious, Biogeography-based optimization-AOMDV-5% Malicious and Biogeography-based optimization-AOMDV- 5% Malicious.

Table I Packet Delivery Ratio for Biogeography-based optimization-AOMDV

Node Pause time (s)	Trust-5% Malicious	Biogeography-based optimization-AOMDV-5% Malicious
10	0.739	0.7794
30	0.8325	0.8853
50	0.8598	0.919
70	0.862	0.9218
90	0.8871	0.946
	Trust-10% Malicious	**Biogeography-based optimization-AOMDV-10% Malicious**
10	0.7221	0.7787
30	0.7895	0.8375
50	0.8401	0.8913
70	0.8421	0.8962
90	0.8101	0.8669

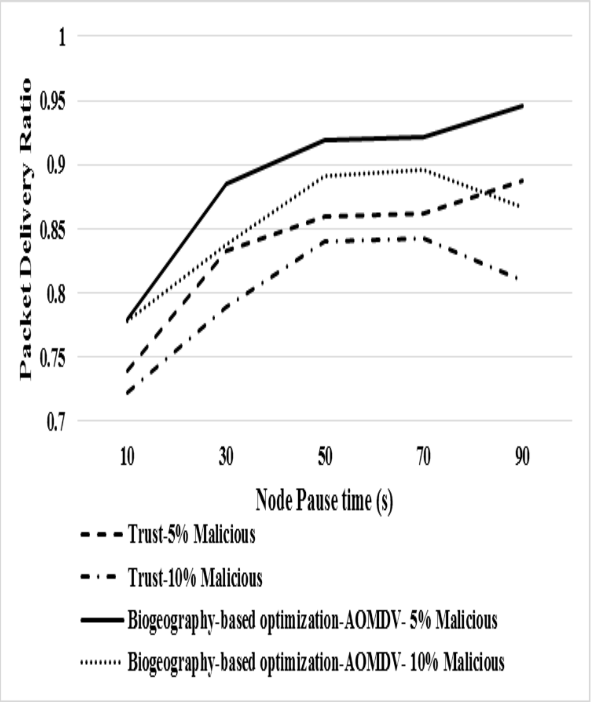

Fig 2 Packet Delivery Ratio for Biogeography-based optimization-AOMDV

From the fig 2, it can be observed that the proposed Biogeography-based optimization-AOMDV- 5% Malicious improved the packet delivery ratio by 5.32%, by 7.63% and by 0.899% than Trust with 5% malicious nodes, Trust with 10% malicious nodes and Biogeography-based optimization-AOMDV- 10% Malicious with node pause time of 10 seconds. The proposed Biogeography-based optimization-AOMDV- 5% Malicious improved the packet delivery ratio by 6.43%, by 15.48% and by 8.73% than Trust with 5% malicious nodes, Trust with 10% malicious nodes and Biogeography-based optimization-AOMDV- 10% Malicious with node pause time of 90 seconds.

Table II Average End to End Delay in second for Biogeography-based optimization-AOMDV

Node Pause time (s)	Trust-5% Malicious	Biogeography-based optimization-AOMDV-5% Malicious
10	0.0086	0.0075
30	0.0014	0.0012
50	0.0014	0.0013
70	0.0012	0.001
90	0.001	0.0009
	Trust-10% Malicious	**Biogeography-based optimization-AOMDV-10% Malicious**
10	0.0144	0.0129
30	0.0047	0.0042
50	0.0031	0.0028
70	0.0014	0.0013
90	0.0012	0.0011

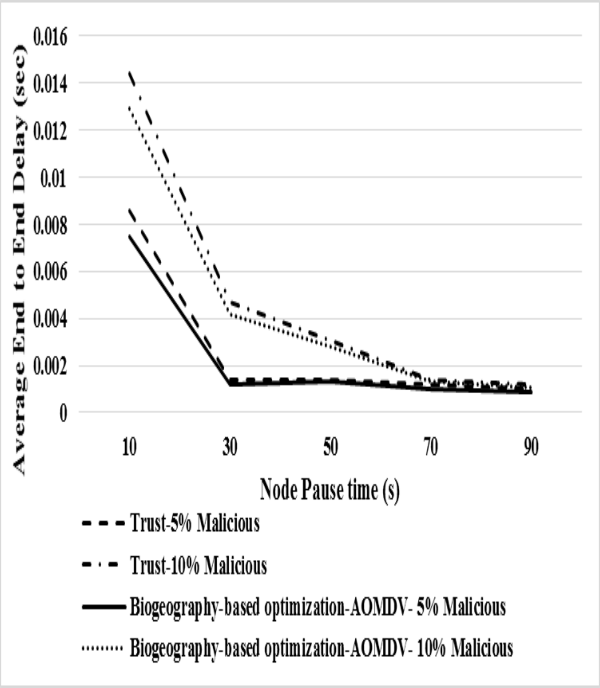

Fig 3 Average End to End Delay in second for Biogeography-based optimization-AOMDV

From the fig 3, it can be observed that the proposed Biogeography-based optimization-AOMDV- 5% Malicious reduced the end to end delay in second by 13.7%, by 63% and by 52.9% than Trust with 5% malicious nodes, Trust with 10% malicious nodes and Biogeography-based optimization-AOMDV- 10% Malicious with node pause time of 10 seconds.

The proposed Biogeography-based optimization-AOMDV- 5% Malicious reduced the end to end delay in second by 10.53%, by 28.6% and by 20% than Trust with 5% malicious nodes, Trust with 10% malicious nodes and Biogeography-based optimization-AOMDV- 10% Malicious with node pause time of 90 seconds.

Table III Average Number of hops to destination for Biogeography-based optimization-AOMDV

Node Pause time (s)	Trust-5% Malicious	Biogeography-based optimization-AOMDV-5% Malicious
10	5.2	5.6
30	5.2	5.5
50	4.4	4.7
70	4.7	5
90	3.4	3.6
	Trust-10% Malicious	**Biogeography-based optimization-AOMDV-10% Malicious**
10	5.8	6.2
30	5.2	5.6
50	4.8	5.1
70	4.7	5
90	3	3.2

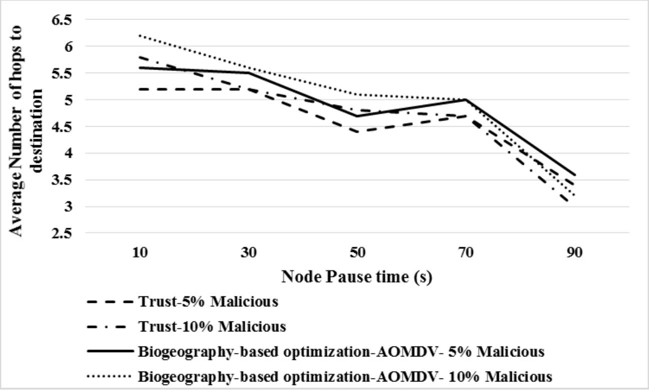

Fig 4 Average Number of hops to destination for Biogeography-based optimization-AOMDV

From the fig 4, it can be observed that the proposed Biogeography-based optimization-AOMDV- 5% Malicious has higher Average Number of hops to destination by 7.41%, but lower Average Number of hops to destination by 3.51% and by 10.2% than Trust with 5% malicious nodes, Trust with 10% malicious nodes and Biogeography-based optimization-AOMDV- 10% Malicious with node pause time of 10 seconds. The proposed Biogeography-based optimization-AOMDV- 5% Malicious has higher Average Number of hops to destination by 5.71%, by 18.2% and by 11.8% than Trust with 5% malicious nodes, Trust with 10% malicious nodes and Biogeography-based optimization-AOMDV- 10% Malicious with node pause time of 90 seconds.

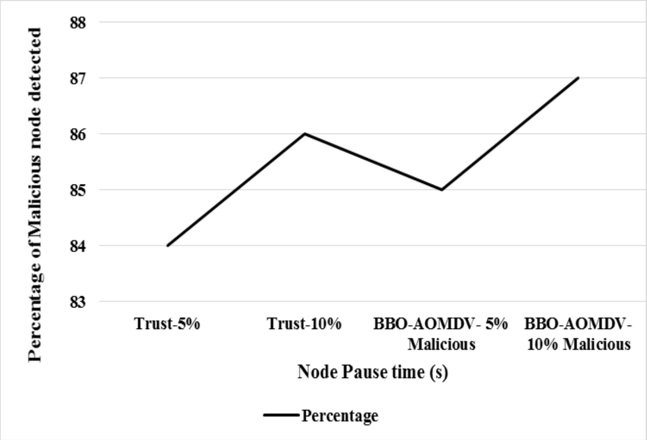

Fig 5 Percentage of Malicious node detected for Biogeography-based optimization-AOMDV

From the fig 5, it can be observed that the proposed Biogeography-based optimization-AOMDV- 10% Malicious has improved Percentage of Malicious node detected by 3.51%, by 1.16% and by 2.33% than Trust with 5% malicious nodes, Trust with 10% malicious nodes and Biogeography-based optimization-AOMDV- 5% Malicious.

V. CONCLUSION

Biogeography-Based Optimization (BBO), is inspired by the science of biogeography, with its own traits exhibiting a large potential in optimization and computation. Results show that the proposed Biogeography-based optimization-AOMDV- 5% Malicious improved the packet delivery ratio by 5.32%, by 7.63% and by 0.899% than Trust with 5% malicious nodes, Trust with 10% malicious nodes and Biogeography-based optimization-AOMDV- 10% Malicious with node pause time of 10 seconds. The proposed Biogeography-based optimization-AOMDV- 5% Malicious improved the packet delivery ratio by 6.43%, by 15.48% and by 8.73% than Trust with 5% malicious nodes, Trust with 10% malicious nodes and Biogeography-based optimization-AOMDV- 10% Malicious with node pause time of 90 seconds.

REFERENCES

1. K., Anuj Gupta, Harsh Sadawarti, (2009). Secure Routing Techniques for MANETs, International Journal of Computer Theory and Engineering (IJCTE), ISSN: 1793-8201, Article No. 74, Vol.1 No. 4, pp. – 456-460.
2. P., Suneja, A.; Kumar, A.; Soni, A., (2015) System Scenario based investigation of AODV and AOMDV Routing Protocol in MANET. International Conference on Soft Computing Techniques and Implementation, pp. 45-48.
3. K., Mahesh, Marina Samir R. Das , On-demand Multipath Distance Vector Routingin Ad Hoc Networks- WIRELESS COMMUNICATIONS AND MOBILE COMPUTING Wirel. Commun. Mob. Comput. 2006; 6:969–988Published online in Wiley InterScience (www.interscience.wiley.com). DOI: 10.1002/wcm.432.
4. K., Selvavinayaki, & E., Karthikeyan. Security Enhanced AOMDV Protocol to Prevent Black Hole Attack in MANET.
5. T., Pandikumar, B., Zewdie, & C.Z., Haile. (2017). Mitigating Black Hole Attack on MANET with AOMDV Protocol. International Journal of Engineering Science, 12666.
6. P., Bansal, & A.K. Gupta, (2014). Impact of Black Hole and Neighbor Attack on AOMDV Routing Protocol. Int. J. Innov. Eng. Technol, 3(4), 90-99.

7. R., Dorai, & M. Rajaram, (2015). Trust and Reputation Mechanism with Path Optimization in Multipath Routing. International Journal of Electrical, Computer, Energitic, Electronic and Communication Engineering, 9(3).
8. R. T., Merlin, & R. Ravi, (2019). Novel Trust Based Energy Aware Routing Mechanism for Mitigation of Black Hole Attacks in MANET. Wireless Personal Communications, 104(4), 1599-1636.
9. W., Guo, M., Chen, L., Wang, Y., Mao, & Q. Wu, (2017). A survey of biogeography-based optimization. Neural Computing and Applications, 28(8), 1909-1926.
10. H., Ma, D., Simon, P., Siarry, Z., Yang, & M. Fei, (2017). Biogeography-based optimization: a 10-year review. IEEE Transactions on Emerging Topics in Computational Intelligence, 1(5), 391-407.
11. F. M. M., Mokbal, K., Saeed, & W. Dan, (2018). Energy Consumption Evaluation of AODV and AOMDV Routing Protocols in Mobile Ad-Hoc Networks. Energy, 9(8).
12. B., Kute, M.; Kharat, (2013). Analysis of Quality of Service for the AOMDV routing protocol. Engineering Technology & Applied Science Research, vol. 3, pp. 359-362.
13. P., Aggarwal, P., Garg, (2016). Aomdv Protocols in MANETS. International Journal of Research in Computer Science & Technology, vol. 4, pp. 3234.
14. W.L., Lim, A., Wibowo,M.I., Desa, & H. Haron, (2016). A biogeography-based optimization algorithm hybridized with tabu search for the quadratic assignment problem. Computational intelligence and neuroscience, 2016, 27

AUTHORS PROFILE

G. Mahalakshmi, Guest Lecturer, Computer Science, Muthurangam Govt. Arts College (Autonomous), Otteri, Vellore - 632 002, priyamahamga@gmail.com.

Dr. A. Suresh: M.C.A., M.Phil., Ph.D., SET. Received PhD in Mobile Computing from Anna University- Chennai. He is now working as Principal, Department of Computer Science in SIRI PSG College of Arts and Science for Women, Sankagiri.asuresh1975@yahoo.com. Work Experience: 20 Years of Experience. Research work related to mobile computing, wireless communication are published in several National and International Journals and Conference.

Retrieval Number: D10521284S519/2019©BEIESP
DOI:10.35940/ijrte.D1052.1284S519

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication