Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 07, July-2020

Bio-Inspired Approach Sybil Attack in AODV based MANET using BFO Algorithm

[1]Ms. S. Swathi
M.Phil, Research Scholar
Department of Information Technology
Bharathiar University
Coimbatore, Tamil Nadu, India

[2]Dr. R. Vadivel
Assistant Professor
Department of Information Technology
Bharathiar University
Coimbatore, Tamil Nadu, India

***Abstract*—Mobile Ad-hoc Network (MANET) is an infrastructure-less network with mobile devices associated remote and it's a self-configuring network without having a fixed framework. MANETs are peer-to-peer, multihop remote systems in which data packets are transmitted in a store and forward way from a source to destination. Bio-Inspired techniques are based on biological principles or models. The objective is to improve the modeling and simulation of the biological framework. Sybil attack could be serious security trouble to be illuminated for the effective delivery of packets in Mobile ad-hoc networks. In this research article focused on, Sybil attack in the AODV routing protocol established on Mobile Ad-hoc Network as well as at that moment optimize it utilizing the Bacteria Foraging Optimization algorithm (BFO) in NS3 simulator utilizing parameter corresponding routing overhead and packet delivery ratio. BFO is a bio-inspired algorithm that simulates bacteria's behavior and can be successfully connected in various areas. Within the conclusion comparison of network nodes with attack and after recompense of attack with BFO has been made. From the results, it has been deduced that BFO works well for the prevention of Sybil attack.**

***Keywords*—MANET, Bio-Inspired, BFO, AODV, Security, Sybil attack**

I. INTRODUCTION

A. MANET

Wireless networks are computer networks that are connected by cables of any kind. The utilize of a wireless network empowers undertakings to maintain a strategic distance from the exorbitant handle of presenting cables into buildings or associations between different equipment areas [1]. The basis of remote systems is radio waves, an execution that takes place on the physical level of network structure. It is found that numerous of the directly existing attacks have a few common highlights and have been categorized into different attacks based on their minor differences. A mobile ad-hoc network is shaped by collecting mobile devices like tablets, Smartphone's, sensors, etc. MANET contains only limited transmission ranges. The ranges represented as the maximum distance between any two nodes such that the signal issue from one node may straightforwardly reach the other node. According to that, the packets are forwarded from any source node to any destination node in a network with the help of multiple hops. Wireless Networks are a connection between different equipment locations.

B. Types of Attack In MANET

Attacks can be classified in many categories like internal attacks, external attacks, active attacks, and passive attacks. Internal Attack This attack usually occurs inside the network. The attacker can regularly include within the communication. A new node that's included in the organization can act as an attacker that has to pick up the get to a network. It has picked up get to the arrange either by making a deal with the current node or by impersonation It is very troublesome to predict the internal attacks as compared to external attacks [2]. External Attack these attacks are used by the person who is outside the network and wants to get access to the network. Active Attack In this attack, an attacker endeavors to modify the information being traded within the network. An Attack may disturb the normal functioning of the networks. The inactive attack, the intruders can modify the packets, inject the packets, drops the packets or it can use the various feature of the network to launch the attack. Passive Attack In this attack, the attacker because it listened or keeps track of data or information that's being traded between two parties. No modification and manufacture are done. Examples of passive attacks are listening in and traffic analysis. The foremost of the attackers are influencing the execution of ad hoc networks and execute malicious activities at the time of sending and accepting the data. The attackers are categorized according to a different layer of the network like a Black-hole attack, a worm-hole attack, a Sybil attack, a jellyfish attack, a gray hole attack, and Rushing attack [3] and so on because the different attacker clashes the organize execution at a different layer.

II. LITERATURE SURVEY

Karuppiah, A. Babu, et al., Sybil nodes can create an arbitrary number of identities but a relationship to non-Sybil nodes. Sybil nodes are ineffectively associated with non-Sybil nodes. One trusted non-Sybil node is known. Based on these suspicions different defense plans such as Sybil guard, Sybil limit, Sybil control, Sybil infer, Sum up, Gatekeeper are proposed. Sybil secure devours less vitality than existing defense components. This arrangement expects that there's an uncommon trusted third party or central specialist, which can confirm the legitimacy of each member, and advance issues certification for the fair one. In reality, such certification can be an extraordinary equipment gadget or an advanced

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 07, July-2020

number. Note that basically both of them are an arrangement of digits, but are put away on distinctive media.

Vasudeva, Amol, et al., proposed ad hoc Sybil identity detection, passive ad hoc Sybil identity with group detection, and energy trust-based system. Specifically, analyze various approaches to mitigate the Sybil attack, focus on eight different techniques to defend a wireless ad hoc network against the Sybil attack. The first scheme uses a trusted center to validate the identity of each pair of nodes that are willing to communicate with each other. A trusted center plays the role of a mediator between two nodes by providing them with a shared secret key to establish a secure link.

A. Security

All networking capacities such as routing and packet sending, are performed by nodes themselves in a self-organizing manner. There are five security goals that need to be known for preventing attacks [4], so as to maintain a reliable and efficient ad-hoc network. The goals to evaluate in MANETs are secure.

1) Authentication

Authentication enables a node to protect the original peer node with whom it is communicating. Authenticity is guaranteed since as it were the authentic sender can deliver a message that will decrypt appropriately with the shared key.

2) Availability

Availability implies the resources are available to authorized parties at suitable times. Accessibility applies both to data and to administrations. It ensures the survivability of network benefits in spite of the denial of service attacks.

3) Non-Repudiation

Non-repudiation ensures that the sender and recipient of a message cannot deny that they have ever sent or received such a message. This can be supportive when have to be separate on the off chance that a node with a few undesired works is compromised or not.

4) Integrity

Integrity implies that resources can be altered as they were by authorized parties or as it were in an authorized way. Alteration incorporates writing, changing status, erasing, and making. Integrity assures that a message being exchanged is never corrupted.

5) Confidentiality

Confidentiality ensures that computer-related resources are gotten to as it were by authorized parties. That's as it were those who should have got to something will really get that access. To maintain the confidentiality of a few private data, to keep them secret from all substances that don't have a benefit to access them. Confidentiality is in some cases called mystery or privacy.

III. AODV ROUTING PROTOCOL IN MANET

Ad-Hoc on Demand Distance Vector (AODV) is a reactive routing protocol that is able to unicast, multicast, and broadcast routing. It is an on-demand routing algorithm, it builds routes between nodes as it were when source hubs requests. It keeps up this way as long as they are required by the sources. The entire path in its header. AODV shapes trees that interface multicast group individuals. The trees are composed of the group individuals and the nodes required associating the individuals. Sequence numbers utilized by AODV to guarantee the freshness of courses. It is self beginning, loop-free, and scales to large numbers of a versatile node. AODV employments the route discovery and course answer handle to form and keep up a course on request. Within the course revelation stage for a source hub to send data to a goal hub, it to begin with first, to begin with, check its possess directing table to see on the off chance that a substantial course exists. In the event that a substantial course does not exist, a source hub broadcasts a worldwide RREQ (Route Request) message that contains the source sequence number, source address, destination sequence number, destination address, broadcast ID, and hop check [5]. The combination of the source address and the broadcast-ID is utilized to extraordinarily distinguish each RREQ message. A hub that gets the RREQ message which is ordinarily the closest hub to the source hub answers quickly with a RREP (Routing Reply) in the event that it contains a fresh route. Otherwise, it advances the RREQ message to set up the course to the goal. The sender chooses the primary node to reply with a RREP. Each RREP control message received, the source node to begin with checks whether it has a section for the goal within the route table or not.

IV. SYBIL ATTACK

Sybil attack shows itself by faking different characters by imagining to be comprising of numerous nodes within the arrange. So one single node can expect the part of multiple nodes and can monitor or hamper numerous nodes at a time. If Sybil attack is performed over a blackmailing attack [6], at that point level of disturbance can be very high. Success in a Sybil attack depends on how the identities are produced within the framework.

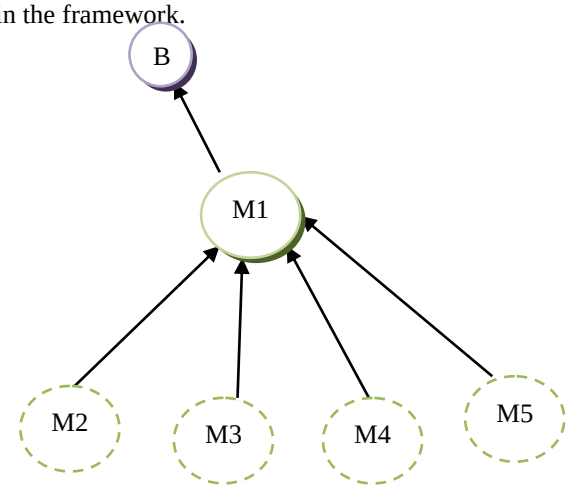

Fig.1. Sybil Attack

In Fig.1 node, M1 assumes compromised nodes identifies of M2, M3, M4, and M5. Node B is a Normal node, M1 is equivalent to those nodes.

A node within the network works different characters effectively at the same time and undermines the authority/power in reputation frameworks. The most point of

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 07, July-2020

this attack is to gain the majority of impact within the network to carry out illegal (concerning rules and laws set within the network) activities within the system. A single entity(a computer) has the capability to make and work different identities [15] (user accounts, IP address-based accounts). To outside observers, these multiple fake identities show up to be real unique personalities.

A. Types of Sybil Attack

- In a direct attack, the honest nodes are affected straightforwardly by the Sybil node(s).
- In an indirect attack, the legitimate node(s) are attacked by a node that communicates specifically with the Sybil node(s). This center node is compromised as it's under the malicious impact of Sybil node(s).

V. BIO-INSPIRED

Bio-inspired implies thoughts inspired by mechanisms or laws working in natural living beings [7]. E.g. Neural Network.

A. Bio-Inspired Networking

Bio-Inspired organizing may be a class of methodologies for productive & versatile organizing beneath uncertain conditions. Communication and administration aspects in organizing are getting to be indeed more challenging in future organizing spaces extending from nanoscale communication systems to interplanetary web. Specialized challenges incorporate the administration of thousands and millions of inter-networking devices that got to be organized using scare resources and troublesome communication channels [8]. The organizing community is creating surprising specialized arrangements. Bio-Inspired organizing may be or perhaps modern one that's rising from early considers into well-understood and carefully examined arrangements E.g. Delay-Tolerant Networking. Bio-Inspired Applications are using in several fields such as Evolutionary Algorithm. An evolutionary algorithm represents a set of search techniques used in computing to find solutions to optimization problems. Artificial Neural Networks (ANN) could be an organization of natural neurons**.** It is non-linear statistical data modeling tools used to acquire knowledge from the environment known as self-learning property. Swarm intelligence is the collective behavior of decentralized, self-organized frameworks. It works based on the ANN system. E.g. Ant/Bee/Termite Colonies, Bacteria Growth, Bird Flocking. Artificial Immune systems are computational frameworks inspired by theoretical immunology and watched immune capacities, standards, and models, which are connected to complex issue domains. Cellular Signaling Pathways is a whole set of cell changes induced by receptor activation is called a signal mechanism or pathway. Cell signaling research includes examining the spatial and worldly elements of both receptors and the components of signaling pathways. A signaling cascade in each target cell coming approximately in a really specific reply which vice versa influences neighboring cells.

VI. BACTERIA FORAGING OPTIMIZATION ALGORITHM

Bacteria foraging optimization algorithms could be a well known computational technique that is base on the think about bacterial foraging behaviors. The complex but organized activities displayed in bacterial foraging designs could inspire a modern arrangement for optimization issues. The underlying mechanism of the survival of microscopic organisms, particularly E. Coli (Escherichia coli) is a type of bacteria that lives within the digestion tracts of healthy people and creatures in a complex environment that has been detailed by researchers within the region of organic sciences. Inspired from these wonders [9] K.M. Passino proposed BFOA was created as a distributed optimization algorithm and controls. In which the self-flexibility of individuals within the bunches looking exercises has pulled in a great bargain of the interface. The classical bacterial foraging optimization frameworks comprise of the guideline mechanisms namely chemotaxis, reproduction and elimination, and dispersal.

A. Use of BFO Algorithm in MANETs

The Bacterial Foraging Optimization Algorithm current researcher using among different bio-inspired calculations and has a place to the field of Microbes Optimization Calculations and Swarm Optimization, and more broadly to the areas of Computational Intelligence and Metaheuristics. It is related to other Swarm Intelligence calculations such as Ant Colony Optimization and Particle Swarm Optimization [10]. It has been utilized in numerous investigate ranges like color pictures quantization, face acknowledgment, building plan issues. On analyzing these problems solution by BFOA, comes about obtained are way better than other bio-inspired and routine approaches. It is computationally successful and faster and understands difficult numerical issues. There have been numerous expansions of the approach that endeavor to hybridize the calculation with other Computational Insights calculations and Metaheuristics such as Genetic Calculation, Molecule Swarm Optimization, and Tabu Search, etc [11]. So motivated by other problem's arrangement and utilizing BFOA in MANETs on AODV convention in this paper and analyze the comes about obtained.

VII. PROPOSED WORK

When the behavior of node changes from its basic nature, it is supposed to be an attack on the network. AODV is one of the finest protocols in MANET which as of now includes a fundamental avoidance conspire against any attack. But when the attack is more irregular and précised in nature at that point it gets to be very troublesome for any convention to deal with it. Sybil attack is one of the most dangerous attacks in terms of its random nature and the ability to bluff the transmitting node. This paper presents the Bacteria foraging optimization algorithm which is based on the AODV protocol to detect Sybil attack is an efficient manner in the whole network. By applying BFO tried to eliminate Sybil nodes from the network through which intermediate network nodes are getting disturbed and that deals with lower energy

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 07, July-2020

consumption and higher packet delivery ratio which increases life span.

A. Steps of Bacterial Foraging Optimization Algorithm

There are three steps in BFOA illustrated as follows:

1. Chemotaxis
2. Reproduction
3. Elimination and Dispersal

1) Chemotaxis

Bacteria generate movement pattern in the knowledge of chemical repellants and attractants are define as chemotaxis. This technique through swimming and tumbling simulates the movement of an E.coli (Escherichia coli) cell via flagella. Biologically an E.coli bacterium can run in two different ways [12]. It can swim or tumble for a period of time in the same direction or alternate for the entire lifetime between these two modes.

2) Reproduction

The population size will remain constant for this process as the healthier bacteria will sexually split up into two bacteria and less healthy bacteria will eventually die which are then situated in the same position [13].

3) Elimination and Dispersal

Events can occur in such a way that all the bacteria can either eradicate or scatter in a region into a new type of the environment. They have both the effect of making a difference and destroying chemotactic advance, since dispersal may put microscopic organisms near extraordinary food sources. In BFO after reproduction processes, the scattering occasion happens in which a few microbes are considered to be killed and moved to another position inside the environment [14]. Fig.2 explains the flowchart of BFOA. This technique consists of three-phase to detect and prevent from Sybil attack in MANET.

Phase 1: Construction of Network

1. Create a network consisting of 50 nodes.

2. Select the source and the destination node.

3. The transmission will begin from source to destination by multi-hop.

4. Get arrange length and width as input.

5. Initialize BFO parameters individual to the network.

Phase 2: Identification of attack

1. Read each node of the population set respective for chemotactic step and so Sybil attack is detected by the chemotactic movement of data in the network and find the cost of location in the network.

2. Perform the next movement respective to swimming and tumbling.

3. Implement the swarming process so node designs can be recognized and calculated. It'll perform comparable courses for transmission. It can be accomplished by transmitting attractant signals to other nodes for finding relative remove between two nodes by utilizing fetched work.

4. The node that is not transmitting the data forward is the Sybil node.

Phase 3: Recovery

1. Implement the reproduction process by performing the splitting of nodes and implement them in the same location with the same route.

2. In the elimination mode of BFOA, eliminate the Sybil node.

3. In the dispersion mode, a node is generated that is the replacement of Sybil node.

4. Evaluate the Packet delivery ratio and the routing overhead.

Below figure.2 flowchart shows the steps of the BFO process.

B. Proposed Algorithm

1. Initialization

2. FOR EACH NODE SYBILHOLE=0;

3. ReceiveReply (Packet P) {

4. if(SYBILHOLE~=1 AND P has an entry in Route Table) {

5. Select Dest_Seq_No from routing table

6. if(p.Dest_Seq_No > Dest_Seq_No) {

7. Generate a tumble angle for the bacterium

8. IF (RREP NOT SENT)

9. THEN SYBILHOLE=1;

10. Else

11. Update the entry position of bacterium of P in the routing table;

12. Unicast data packets to the route specified in RREP

13. else {

14. discard RREP

15. } }

16. else {

17. if(P.Dest_Seq_No >= Src_Seq_No) {

18. Make entry of P in the routing table

19. }

20. else }

21. discard this RREP

22. }}}

23. end

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 07, July-2020

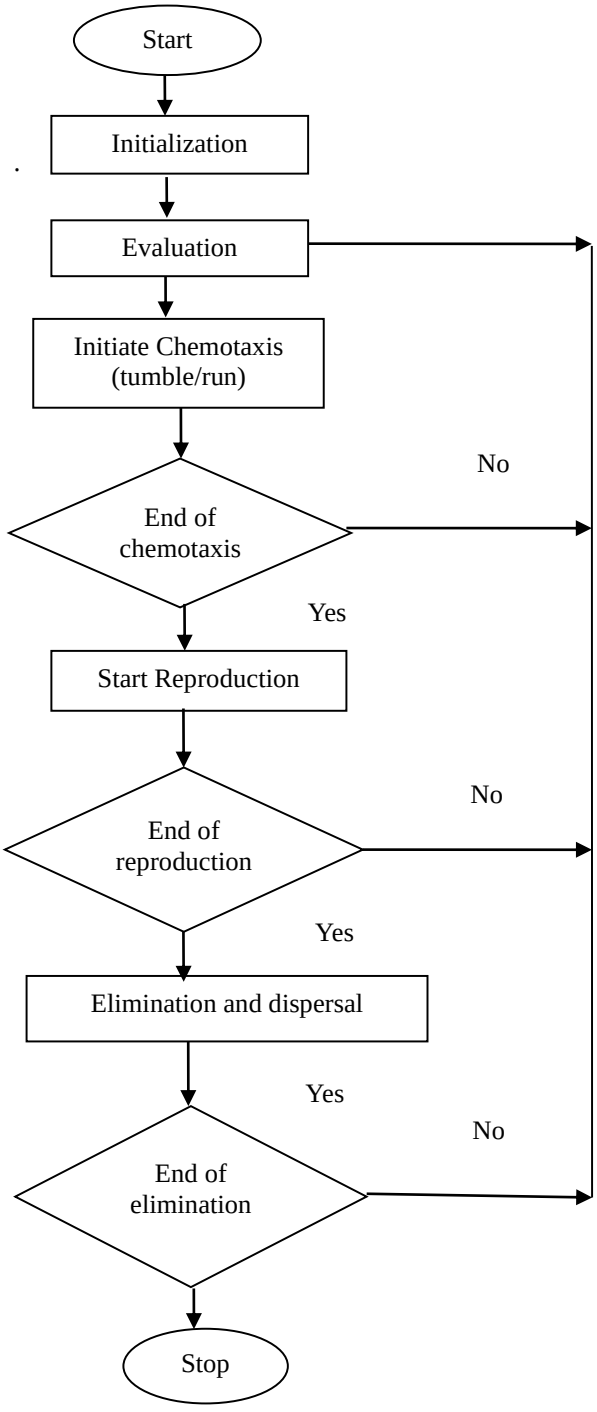

Fig.2. Flowchart of BFO

VIII. RESULTS AND IMPLEMENTATION

A. Routing overhead with Sybil attack

The below figure.3 appears the routing overhead compensation with a Sybil attack. Routing overhead is the parameter in which packets during sending get the problem in routing from source to destination. It has been seen that the esteem of routing overhead is on a high level. In this situation, a malicious node is inserted into the arranging and attacks the network and directing overhead happens.

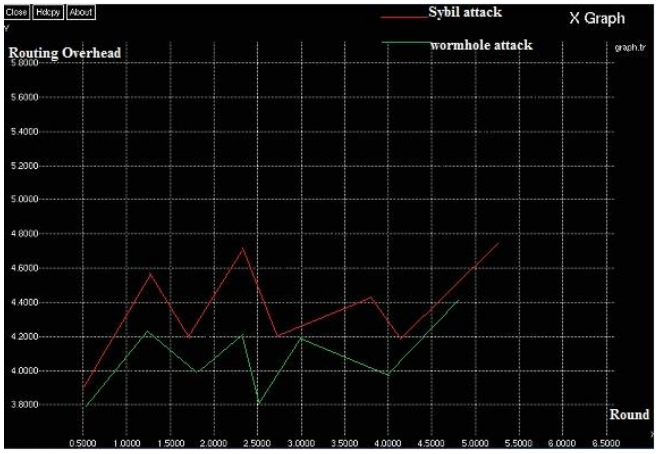

Fig.3. Routing overhead with Sybil attack

B. Routing overhead using BFO

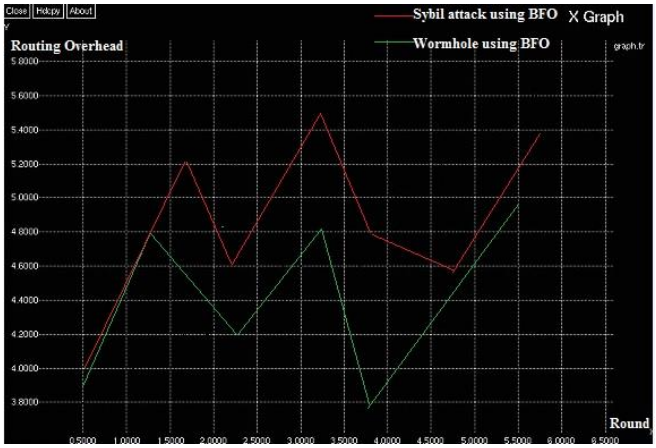

Fig.4 Routing overhead using BFO

The Above figure.4 shows routing overhead compensation with BFO. Routing overhead is the parameter in which packets during sending get the problem in directing from source to destination. Routing overhead must be low in arrange to have efficient comes about. So, with the utilization of optimization algorithm BFO, routing overhead has been decreased value. Hence BFO works well in the optimization of routing over the head in organize.

C. Packet delivery ratio with Sybil attack

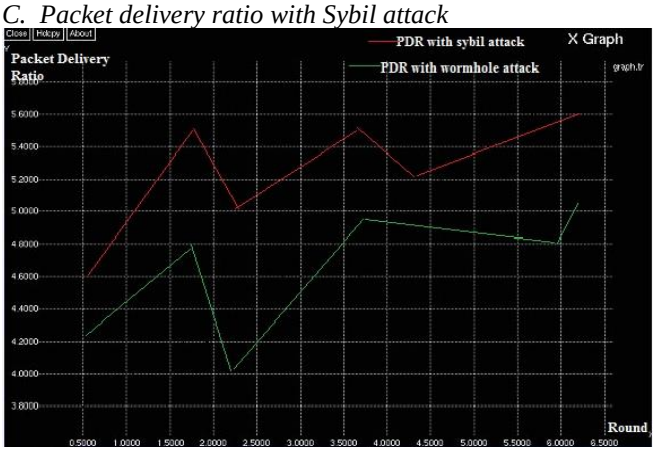

Fig.5 Packet delivery ratio with Sybil attack

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 07, July-2020

The Above figure.5 shows the packet delivery ratio with the Sybil attack. It is characterized as the ratio of data packets received by the goal of those generated by the source.

Packet Delivery Ratio = (no.of packets sent – no.of packet dropped) / total no.of packets sent.

It has been seen that the packet delivery ratio has been decreased by Sybil attack in organizing. As packets are sent continually, they will reach after some time delay to goal and a few packets are drop between nodes. As circular of node increases, the packet dropping is additionally incrementing.

D. Packet delivery using BFO

Fig.6 packet delivery ratio using BFO

The Above figure.6 shows packet delivery ration using BFO. The ratio of data packets received by the goals to those generated by the sources. The Packet delivery ratio must be high within the organization. From the simulation graph, it has been seen that the Packet delivery ratio has been improved to a greater rate in comparison to the presence of an attack. So after compensation with BFO packet delivery ratio increments or it has been enhanced.

IX. CONCLUSION AND FUTURE SCOPE

This paper analyzes the performance of the BFO technique in MANETs. The node's movements are the same as the bacteria movement. This technique is applied for detection and prevention from Sybil attack which can be easily applied MANET. In a Sybil attack, one single node can expect the part of multiple nodes and can monitor or hamper numerous nodes at a time. By applying the BFO technique on MANETs gets better results than existing techniques. This improves the performance in terms of routing overhead attack after routing overhead in BFO, packet delivery ratio after compensation with BFO increases. For future scope, this topic can do a hybridization of BFO with the Genetic Algorithm and then compare it with this outcome.

REFERENCES

[1] Parul Gupta "A Literature Survey of MANET", International Journal of Engineering and Technology, Vol.03, Iss.02, Feb 2016.
[2] K. Rajkumar and S. Prasanna "Complete Analysis of Various Attacks in MANET", International Journal of Pure and Applied Mathematics, Vol.199, No.15, 2018.
[3] P. Narendra Reddy, CH. Vishnuvardhan and V. Ramesh, "Routing Attacks in Mobile Ad-Hoc Networks" International Journal of Computer Science and Mobile Computing, Vol.2, Iss.5, Pg.360-367, May 2013.
[4] Priyanka Goyal, Sahil Batra and Ajith Singh "A Literature of Security Attack in Mobile Ad-Hoc Networks", International Journal of Computer Applications, Vol.9 Iss.12, Nov 2010.
[5] Puneet Kaur and Navdeep Kaur, "A Survey of Black-Hole Attack In Aodv", International Journal of Advanced Computronics and Management Studies", Vol.1, Iss.2, pp.11-15, Mar 2016.
[6] Mr. A. Babu karuppiah and A. Raja Prakash, "Sybilsecure: An Energy Efficient Sybil Attack Detection Technique In Wireless Sensor Network", International Journal of Information Sciences and Techniques, Vol.4, No.3, May 2014.
[7] L.J.G. Villalba and D.R. Canas, "Bio-Inspired protocol for MANET", Vol.4, Iss.18, p.2187-2195, Dec 2010.
[8] F. Dressier and O.B. Akan, A Survey of Bio-Inspired Networking, Comp. Net., Vol.54, Iss.6, pp.881-900, Apr 2010.
[9] Preeti Gulia and Sumita Sihag, Enhance Security in MANET using Bacterial Foraging Optimization Algorithm", International Journal of Computer Applications, Vol.84, Iss.1, Dec 2013.
[10] Vipul Sharma, S.S. Patnaik and Tanuj Garg, "A Review of Bacterial Foraging Optimization and Its Applications", International Journal of Computer Applications, 2012.
[11] Kanika Arora and Sonia Jindal, "Bacteria Foraging Optimization against Worm-Hole attack in AODV Based MANET", International Journal of Innovative Science, Engineering & Technology, Vol.2, Iss.9, Sep 2015.
[12] R. Vijay, Intelligent Bacterial Foraging Optimization Technique to Economic Load Dispatch Problem", International Journal of Soft Computing and Engineering, Vol.2, Iss.2, May 2012.
[13] Kanika Bawa and Shashi B. Rana, "Prevention of Black-Hole Attack in MANET using Addition of Genetic Algorithm to Bacterial Foraging Optimization", International Journal of Current Engineering and Technology, Vol.5, No.4, Aug 2015.
[14] Aruna and Vikas Gupta, "Soft Computing Implementation for Mobile Ad-Hoc Network using Bacteria Foraging Optimization Algorithm", International Journal of Computer science and Communication Engineering, Vol.2, Iss.2, May 2013.
[15] Vasudeva Amol and Manu Sood "Survey of Sybil attack Defense mechanism in wireless ad hoc networks" Journal of network and Computer Applications, Vol. 120, No. 78-118, Oct 2018.