I J C T A, 9(25), 2016, pp. 113-121 ISSN: 0974-5572

Detection of Black Hole Attack In Mobile AD-HOC Networks Using Hybrid Glowworm Swarm Optimization (HGSO) Algorithm with Artificial Fish Swarm Algorithm (AFSA)

R. Vijayakumar* and K.R. Shankar Kumar**

ABSTRACT

A mobile ad-hoc network is a group of mobile nodes which can communicate between them without the help of any centralized infrastructure. It consists of number of mobile nodes with exceptional quality of self-managing and self-organizing network. Military operations and disaster management are the important applications of MANET. In preventing routing attacks routing protocols plays a significant role. Security attacks can be initiated towards any layer of the stack protocol. MANET'S distinctive characteristic like dynamic network topology, battery power and limited bandwidth makes routing a challenging task. Several researches are done in this area and many efficient routing protocols were proposed. But due to the presence of malicious node, these protocols are vulnerable to attacks. Therefore for establishing the attractive MANET, security is a major concern. In this work, hybrid swarm intelligence algorithms are employed to overcome the drawbacks of the previous approaches. Here, proposed a Hybrid Glowworm Swarm Optimization (HGSO) algorithm with Artificial Fish Swarm Algorithm (AFSA). This hybrid algorithm has immediate convergence and searching potential to solve the routing complication effectively. This modified protocol is compared with existing protocol by using various parameters i.e. packet delivery ratio, end-to-end delay and throughput. The results shows to increase in packet delivery ratio, throughput and decrease in end-to end delay show better performance of proposed work as compared existing.

1. INTRODUCTION

In recent years, Mobile Ad-hoc Network (MANET) comprises different wireless mobile nodes which are communicating with each other to form network. MANET is a collection of wireless mobile nodes forming temporary network and it does not have permanent infrastructure therefore it is called as infrastructure-less network [1]. Infrastructure less networks has no fixed routers; all nodes are capable of movement and can be connected dynamically in an arbitrary manner. Nodes of these networks function as routers which discover and maintain routes to other nodes in the network.

In Mobile Ad hoc Networks (MANET) each node has limited wireless transmission range, so the routing in MANETs depends on the cooperation of intermediate nodes. Two types of routing protocols have been defined for ad hoc networks: Table-driven protocol and On-demand routing protocol. Table driven protocols are proactive in nature and consume excessive network bandwidth. On the other hand, on demand routing protocol can exchange routing information only when needed. Ad-hoc On demand Distance Vector (AODV) [2] routing protocol is an on demand routing protocol that focuses on discovering the shortest path between two nodes with no consideration of the reliability of a node. The structure of an Ad-hoc network leads to some special kinds of attacks especially attacks on the connectedness of the network.

* Assistant Professor, Department of Computer Science and Engineering, Sri Ramakrishna Engineering College, Coimbatore, Tamilnadu, India, *Email: vijayakumar.r@srec.ac.in*

** Professor, Department of Electronics and Communication Engineering, Ranganathan Engineering College, Coimbatore, Tamilnadu, India, *Email: shanwire@gmail.com*

Most ad hoc routing protocols rely on implicit trust-your-neighbour relationship to route packets among participating nodes. This naive trust model allows malicious nodes and selfish nodes to paralyze the network. Selfish nodes do not directly damage other nodes but their effect cannot be underestimated. Security in the routing protocol is necessary in order to guard against these attacks but relatively little work has been done in securing ad hoc network routing protocols. Secure ad hoc network routing protocols are difficult to design, due to the high dynamic nature of the network. Some protocols have been proposed to secure the network from these attacks. Some of these protocols handle attacks by malicious nodes but not the selfish nodes and some handle selfish nodes nicely but malicious nodes not so nicely.

Routing in mobile ad hoc network faces additional problem and challenges when compared to routing in wired network with fixed infrastructure. There are different type of protocols have been developed to defend against various attacks on Mobile ad hoc network. The problem of routing face some factors such as low bandwidth, dynamic topology, high power consumption and high error rates. Dynamic Source Routing (DSR) protocol is a reactive protocol i.e. it determines the proper route only when a packet needs to be forwarded. The node flood the network with a route request and builds the required route from the responses it receives [3]. Destination-Sequenced Distance-Vector (DSDV) routing protocol is a proactive table driven algorithm based on classic Bellman-Ford routing. In proactive protocols, all nodes learn the network topology before a forward request comes in [4]. Hybrid routing protocol such as Zone Routing Protocol (ZRP) which is a protocol that initiates the route-determination procedure on-demand, but at limited search cost [5].

Swarm Intelligence (SI) is the collective behaviour of decentralized, self-organized systems, natural or artificial. The expression was introduced by Gerardo Beni and Jing Wang in 1989, in the content of cellular robotic systems [6]. The inspiration often comes from nature especially biological systems. Principle of SI is a multi-agent system that has self-organized behaviour that shows some intelligent behaviour. Bonabeau [7] provide the following definition of swarm intelligence: "Swarm Intelligence (SI) is the properly of a system whereby the collective behaviour of (unsophisticated) agent interacting locally with their environment cause coherent functional global patterns to emerge".

Nature's self-organizing systems, such as insect societies, termite hills, bee colonies, bird flocks and fish schools, provide precisely these features and hence have been a source of inspiration for the design of many routing algorithms for MANETs [8]. Out of all the techniques inspired by Hybrid Glowworm Swarm Optimization (HGSO) algorithm with Artificial Fish Swarm Algorithm (AFSA) algorithms have evolved as a promising solution for efficient routing in MANETs. In recent years models of collective intelligence of bacteria have been transformed into useful optimization algorithms. For last many years, swarm based algorithms have captivated the researchers for solving routing problem in MANETs. Many algorithms have been proposed by researchers in last few years and many more are in pipeline.

2. RELATED WORK

Al-Shurman et al. [9] presented on-demand distance vector (AODV) protocol to handle the black hole attack. It is used to find more than one route to the destination and also to exploit the packet sequence number included in any packet header. This solution provides a fast and reliable way to identify the suspicious reply. No overhead will be added to the channel because the sequence number itself is included in every packet in the base protocol. However it has issue with handling of group attacks.

Cai et al. [10] introduced a method to detect black-hole and gray-hole attacks in ad hoc network. The authors have proposed a path-based method that overhears the next hop's actions. As the scheme does not send out control messages it saves the system resources. To lower the false positive rate under high network overload, a collision rate reporting system is established in the Media Access Control (MAC) layer. This adaptive threshold approach decreases the false positive rates.

Sharma et al [11] proposed a method to defend against the wormhole attack. In the proposed solution the authors use digital signatures to prevent against the wormhole attack. Whenever a node wants to send a packet it initiates RREQ. Along with RREQ it also sends its digital signature. The nodes in the network verify this digital signature with the one stored in their database and if there is match, they confirm that the RREQ is from a legitimate source. The malicious node replaying the RREQ either has a signature of other node or does not have any and hence is identified and isolated from further transmission.

Das et al [12] discussed about security issues in MANET. An algorithmic approach is to focus on analysing and improving the security of Ad-hoc On-Demand Distance Vector (AODV), which is one of the popular routing protocols for MANET. Our aim is on ensuring the security against Black hole attack. The proposed solution is capable of detecting & removing Black hole node(s) in the MANET at the beginning. Also the objective of this paper is to provide a simulation study that illustrates the effects of Black hole attack on network performance.

Raj et al [13] presented Detection, Prevention and Reactive AODV (DPRAODV) to prevent security threats of black hole by notifying other nodes in the network of the incident. The simulation results demonstrate that our protocol not only prevents black hole attack but consequently improves the overall performance of (normal) AODV in presence of black hole attack. However it still has issue with delay performance.

Sen et al [14] presented defense mechanism for dealing with black hole attack. In this research, routing security issues in MANETs are discussed and the cooperative black hole attack has been described. A security protocol has been proposed that can be utilized to identify multiple black hole nodes in a MANET and thereby identify a secure routing path from a source node to a destination node avoiding the black hole nodes.

3. BLACK HOLE ATTACK

A packet drop attack is one of the most common type of network layer attack [15]. It is also called as Black hole attack. In this, the intruder displays a least hop count value and the source node then routes the packets through this compromised node. The malicious node then drops the packets. This type of attack leads to extensive loss of information transmitted. The attack is illustrated in the Fig.1.

In Fig.1, the source node A wants to send data to the destination node D and this initiates the route discovery process. So if malicious node C claims to have the shortest route to destination as soon as it receives the RREQ from source A. It will then send a response to A before other nodes. Hence, node A will start to route all data through C ignoring other responses from the neighbouring nodes. This node C then will drop the packets upon receiving them.

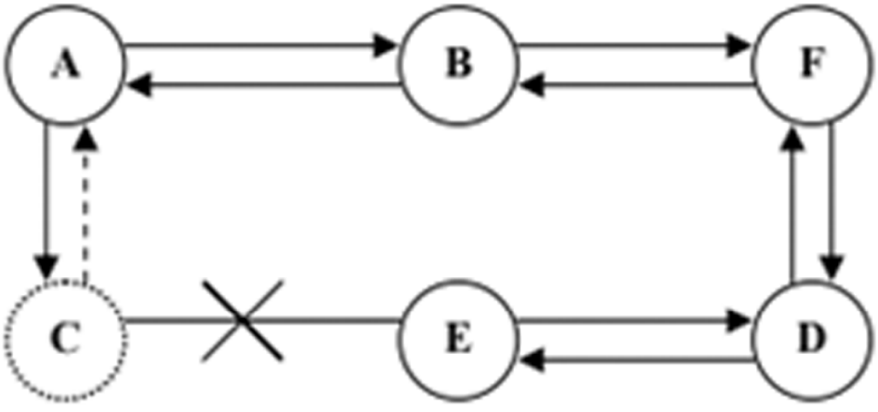

Figure 1: Black Hole Attack

4. PROPOSED METHODOLOGY

The proposed technique can be used to identify black hole nodes after optimizing the location of BS and then transmitting data packets to that SN in its neighbourhood which can actually send the data further to the BS. We make use of control packets including encryption key for this task. First, RREQ is broadcasted in the network. As, black hole nodes use tiny OS beaconing protocol like other normal nodes to form the part of routing tree, they are the first one to send reply without checking their routing table, advertising that they have the shortest route towards the destination. So, in the broadcasting mode, reply comes from both black hole and non-black hole nodes present in its neighbourhood. Now, control packets with encryption keys are sent to the preferable nodes. If RRPLY comes from any node, then data packet is transmitted to it. In case, nodes do not respond to source SN, then they can be considered as black hole nodes. It is to be noted that, the data packet is dropped only when there is no non-black hole node available in the neighbourhood of the source SN. This procedure is performed in the network at regular intervals of time to identify the presence of a black hole region.

4.1. Proposed GSO–AFSA Process

In the basic GSO algorithm, each glowworm only in accordance with Lucifer in values of glow-worms in its neighbour set, selects the glowworm by a certain probability and moves towards it. However, if the

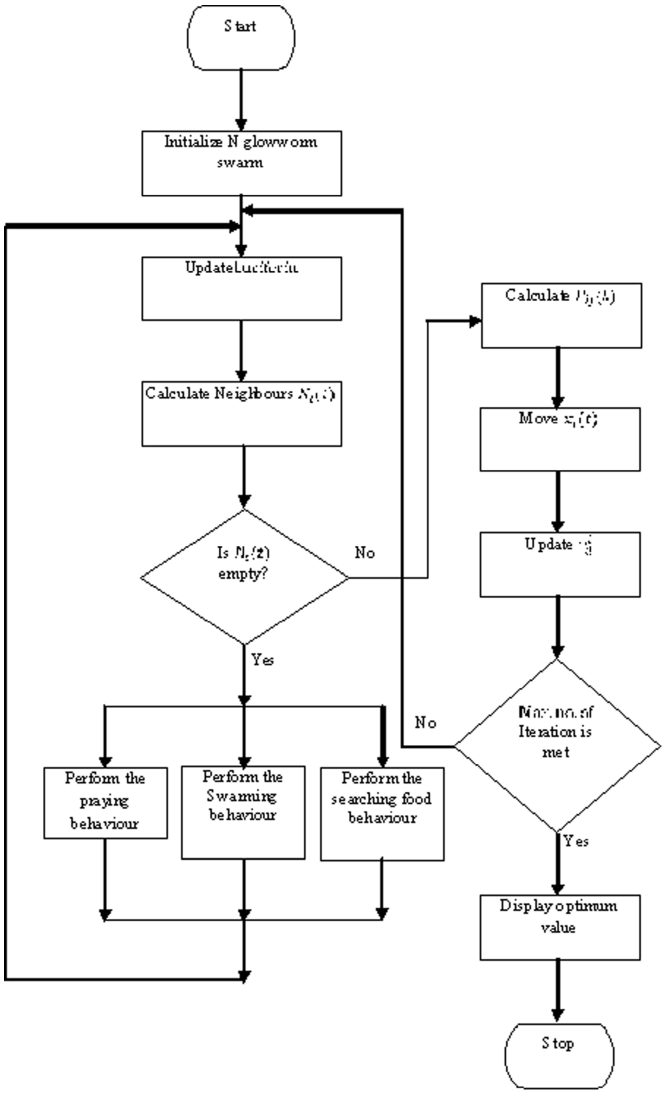

Figure 2: Flowchart for GSO-AFSA

search space of a problem is very large or irregular, the neighbour sets of some glowworms may be empty, which leads these glow-worms to keep still in iterative process. To avoid this case and ensure that each glowworm keeps moving, predatory behaviour of AFSA into GSO is introduced in this work and proposes Hybrid GSO (HGSO) algorithm is proposed. The idea of HGSO is as follows: the glowworms whose neighbour sets are empty are carried out predatory behaviour in their dynamic decision domains. Assume that N represents population size, $x_i(t) = \left[x_i^{(1)}(t), x_i^{(2)}(t), \ldots x_i^{(d)}(t) \right]$ denotes the position of the *i*-th glowworm at the t-th iteration. The flowchart is shown in Figure 2.

The procedure of GSO-AFSA can be described as follows:

Step 1: Let $l_i(0) = l_0, r_d^i(t) = 0$; here, t denotes the number of GSO iterations. The position $x_i(t)$ (i - *1*; 2, ..., N) of each glowworm in the search space is randomly initialized. Fitness value $f(x_i)$ of each glowworm is calculated. The current optimal position x' and the current optimal value $f_x^{'}$ according to the fitness values is initialized .

Step 2: The Lucifer in value $l(t)$ of each glowworm is updated according to (5.11)

Step 3: $N_i(t)$ and $P_{ij}(t)$ for each glowworm is calculated according to (5.12) and (5.13).

Step 4: For each glowworm, if $N_i(t)$ is not empty, then according to $P_{ij}(t)$ and roulette method, the j-th glowworm in $N_i(t)$ is selected and move toward it, $x_i(t+1)$ is calculated according to (5.14), Or else, otherwise, $x_i(t)$ is used as the initial point AFSA behavior in $r_i^d(t)$ and $x_i(t+1)$ is got. If $x_i(t+1) < q$, then $x_i(t+1) = a_j$; If $x_i(t+1) > b_j$, then $x_i(t+1) = b_j$, where $j = 1, 2, \ldots, d$.

Step 5: The current fitness value $f(x_i(t+1))$ of each glowworm is calculated, if the optimal position and optimal value of the current population are better than x^* and f_x^*, then x^* and f_x^* is updated or else, it is not update.

Step 6: If the maximum number of iterations is met, x^* and f_x^* then stop and output x^* and f_x^*; or else, $r_i^d(t+1)$ is calculated according to (5.15) and let $t = t + 1$, returned to Step 2.

4.2. Proposed GSO–AFSA Process to Detect the Attack in MANET

The working principles of the algorithm are given below:

1. Establish a network with N number of nodes.
2. Specify the properties of network.
3. Define the source and the destination node over the network.
4. Place the glowworm at each node in the network.
5. Define the m malicious nodes over the network.
6. Route discovery process: Source node broadcast the RREQ message to neighboring nodes using glowwormtechnique.
7. Collecting replies:
   - Collecting the neighboring nodes information stored in routing table.
   - Neighboring nodes receive the request then it will check whether the node is destination or not.

If yes then

glowwormis sent to only that neighbor

Else

it's forwarded to all the neighbors.

A node is receiving a glowwormfor the first time, will create a record in its routing table and fields such as destination address, next fitness value.

8. For each glowworm(currently in node i)

   Do

   - Choose the neighbor node, probability value will be high that route/neighbor needs to be considered.
   - Add that node pheromone value to neighboring pheromone table with the node, fitness objective value between these nodes until the glowwormhas reached the destination.

   End

9. The full process is mention above to get repeated until the glowwormreaches the destination node.
10. When glowwormdestroy, it is reaches to the destination and create another back glowworm send to along the path to the source node. It is an agent that establishes the fitness value to the destination.
11. Route maintenance: Once forward glowwormand backward glowworm have established route path between source to destinations and data packets are send along the same path. The fitness value is strengthened means path is shortest path between these two nodes.

5. Result and Discussion

The experimental results were implemented in Ns2 Simulator and the result is compared. The proposed methodology is compared with the existing algorithm of safe route method based upon the hybrid swarm based routing algorithm on the basis of throughput, packet delivery ratio, end-to-end delay and so on. The performance and results of the routing algorithm as below:

5.1. Throughput

The throughput is the number of bytes transmitted or received per second. The throughput is denoted by T, Throughput = received node/simulation time

$$T = \frac{\sum_{i=1}^{n} N_i^r}{\sum_{i=1}^{n} N_i^S} \times 100\%$$

Where, N^r = average receiving node for the ith application, N^s = average sending node for the ith application, and n = number of applications. In Figure 3 shows that the proposed algorithm improved good throughput compared to AODV with black hole attack.

5.2. Packet Delivery Ratio

It can be measured as the ratio of the received packets by the destination nodes to the packets sent by the source node. PDR = (number of received packets / number of sent packets) * 100

Where, N^s, N^r node sent by the sender and the number of application data node received by the receiver, respectively for the ith application, and n is the number of applications.

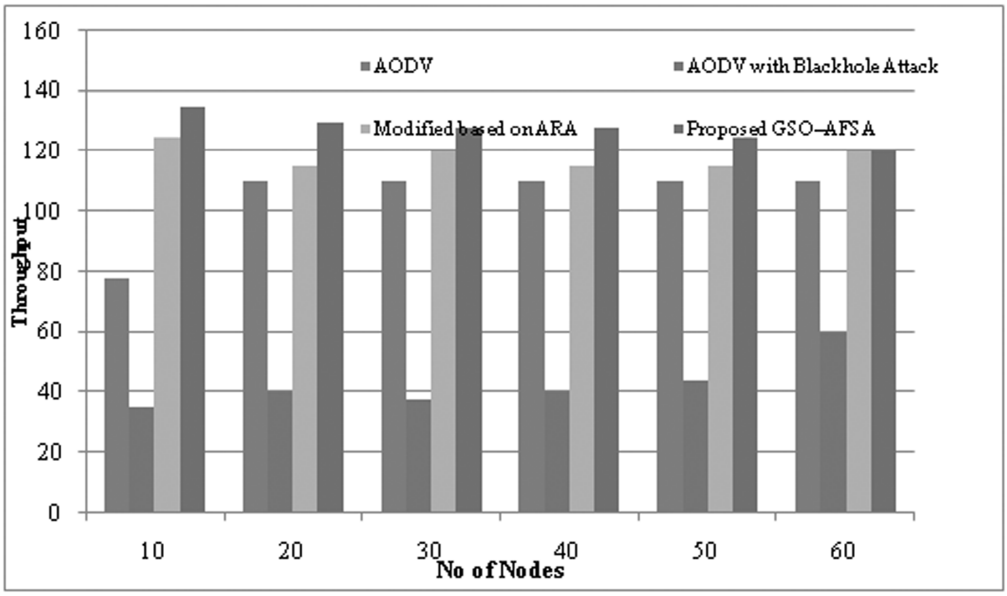

Figure 3: Throughput Comparison

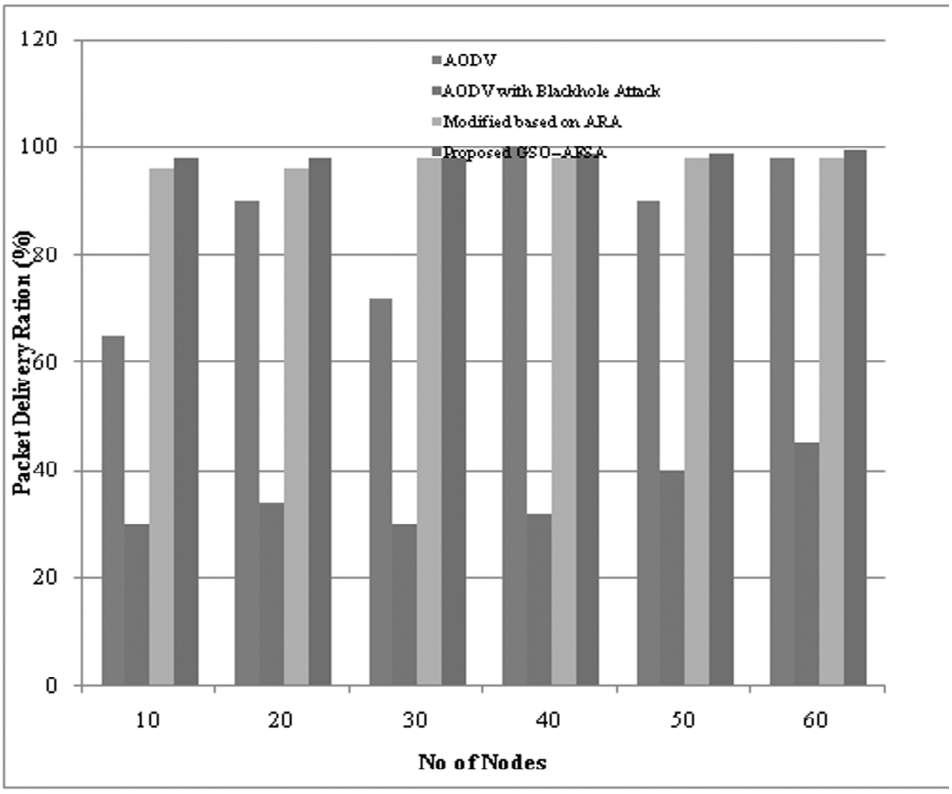

Figure 4: Packet Delivery Ration Comparison

In Figure 4 shows that packet delivery ratio of the proposed algorithm is more than AODV routing algorithm with black hole attacks. Black hole stimulate packet dropping, the original AODV decreases packet delivery ratio with increase in number of nodes.

5.3. End-to-End Delay

It represents the time required to move the packet from the source node to the destination node. E-2-E delay [packet_ id] = received time [packet_ id]– sent time [packet_ id]

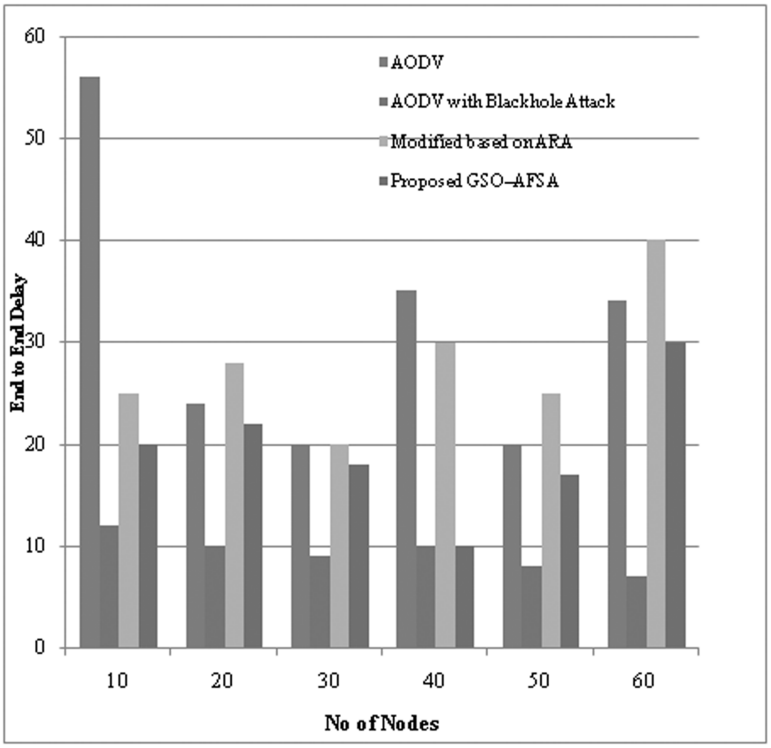

Figure 5: End-to-end Delay Comparison

The average end-to-end delay can be calculated by summing the times taken by all received packets divided by its total numbers.

$$D = \frac{\sum_{i=1}^{n} d_i}{n}$$

Where, d_i = average end to end delay of node of ith application and n = number of application.

In Figure 5 shows that the proposed algorithm provided minimum end-to-end delay compared with original AODV with black hole attack.

6. CONCLUSION

This paper discusses about Mobile Ad Hoc Networks which initiate that most repeated attack is a black hole in MANETs. To discover a resolution for that various algorithms are available. But to decide security and performance issues some improvements on the routing technique is implemented. We are analyzed the effects of black hole attack in the light of network load, throughput and end-to-end delay in MANETs and simulating the black hole attack using reactive routing protocols (e.g. AODV). Compared and observed that AODV without attack gives better result in all situations. After observing the results it is found that under attack case system has more packet drop ratio it is always greater to threshold. Design and implement a security algorithm for detection of black hole attack based on Ad hoc On-Demand Distance Vector routing protocol and Artificial Fish Swarm Algorithm (AFSA) into Glowworm Swarm Optimization (GSO) algorithm. Implementation of proposed method is quite efficient for network and able to detect attack. In addition, the performance of the network is improved effectively. The summary of performance is packet delivery ratio, end-toend delay and throughput can be improved. The proposed protocol can able to improve two main problems such as security and performance, into one place, but this concept is able to detect only one attack and effective for black hole. In future a framework for security is required, where more than one attack are handled.

REFERENCES

[1] Asma Adnane, Christophe Bidan and Rafael Timóteo de Sousa Júnior, "Trust-based security for the OLSR routing protocol," Computer Communications, Vol. 36, No. 10-11, June 2013.

[2] Charles E. Perkins, Elizabeth M. Belding Royer and Samir R.Das, "Ad-hoc On-Demand Distance Vector(AODV) Routing," Mobile Adhoc Networking Working Group, Internet Draft, February 2003.

[3] David B. Johnson, David A. Maltz and Yih-Chun Hu, "The Dynamic Source Routing (DSR) Protocol for Mobile Ad Hoc Networks," http://www.ietf.org/internetdrafts/draft-ietf-manet-dsr-10.txt, July 2004

[4] Charles E Perkins and PravinBhagwat, "Highly Dynamic Destination Sequenced Distance Vector Routing (DSDV) for Mobile Computers," SIGCOMM 94, Pp. 234-244, 1994.

[5] Haas, J.Zygmuntand Marc R. Pearlman, "The performance of query control schemes for the zone routing protocol," IEEE/ACM Transactions on Networking (TON) 9(4), pp. 427-438, 2001.

[6] G. Beni and J. Wang, "Swarm intelligence in cellular robotic systems," Proceedings of NATO Advanced Workshop on Robots and Biological Systems,;Tuscanty, Italy, 1989.

[1] http://en.wikipedia.org/wiki/swarm_ intelligence

[8] AMAbdel-Monien and A.Hedar, "An Ant Colony Optimization algorithm for the Mobile Ad hoc network Routing problem based on AODV protocol," 10th International Conference on Intelligent Systems Design and Application, pp. 1332– 7, 2010

[9] Al-Shurman, Mohammad, Seong-Moo Yooand Seungjin Park, "Black hole attack in mobile ad hoc networks," Proceedings of the 42nd annual Southeast regional conference. ACM, 2004

[10] Jiwen CAI, Ping YI, Jialin CHEN, Zhiyang WANG and Ning LIU, "An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network," 24th IEEE International Conference on Advanced Information Networking and Applications (AINA),Perth, Australia, pp. 775- 780, 2010

[11] Pallavi Sharma and AdityaTrivedi, "An Approach to Defend against Wormhole Attack in Ad Hoc Network Using Digital Signature," IEEE 3rd International Conference on Communication Software and Networks (ICCSN), Pp.307-311, 2011.

[12] Das,Rajib, BipulSyamPurkayasthaand Prodipto Das, "Security Measures for Black Hole Attack in MANET: An Approach," arXiv preprint arXiv:1206.3764 , 2012.

[13] Raj, N.Payal and Prashant B. Swadas,"Dpraodv: A dyanamic learning system against blackhole attack in aodv based manet," arXiv preprint arXiv:0909.2371, 2009.

[14] Sen, Jaydip, SripadKoilakondaand ArijitUkil, "A mechanism for detection of cooperative black hole attack in mobile ad hoc networks," IEEE. Second International Conference on Intelligent Systems, Modelling and Simulation(ISMS),2011.

[15] K. Vishnu and Amos J Paul, "Detection and Removal of Cooperative Black/Gray hole attack in Mobile ADHOC Networks," International Journal of Computer Applications , 2010.