Australian Journal of Basic and Applied Sciences, 9(10) Special 2015, Pages: 31-38

ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

SABC-AODV A Secure Routing Protocol to Mitigate Blackhole Attack in Manet using Artificial Bee Colony Optimization

[1]M. Vijay Anand and [2]C. Jayakumar

[1]*Professor, Department of Computer Science and Engineering, Aksheyaa College of Engineering, India.*
[2]*Professor, Department of Computer Science and Engineering, RMK Engineering College India.*

ARTICLE INFO

Article history:
Received 28 January 2015
Accepted 25 February 2015
Available online 6 March 2015

Keywords:
MANET, AODV, SABC-AODV, Black Hole Attack.

ABSTRACT

Mobile ad hoc networks (MANETs) are multi-hop wireless networks of mobile nodes constructed dynamically without the use of any fixed network infrastructure. The major issue related with the MANET is its mobility, unplanned topology change, energy and its edifice system. This paper proposes a modified bio-inspired routing protocol called SABC-AODV (**S**ecure **A**rtificial **B**ee **C**olony – AODV) for secured routing of data in Manet. It uses the methodology of artificial bee Colony algorithm and AODV protocol. The Proposed scheme is efficient as it uses a novel combination of group signature and ID-based encryption for route discovery. The simulation results stands good for increased packet delivery ratio and reduced end to end delay in Manet and also mitigates the Black hole attack.

To Cite This Article: M. Vijay Anand and C. Jayakumar., SABC-AODV A Secure Routing Protocol to Mitigate Blackhole Attack In Manet using Artificial Bee Colony Optimization. ***Aust. J. Basic & Appl. Sci.,*** *9(10): 31-38, 2015*

INTRODUCTION

A Mobile Adhoc Network is a collection of self-determining mobile nodes that can communicate to each other via radio waves. The mobile nodes that are in radio range of each other can directly communicate, whereas others need the aid of intermediate nodes to route their packets. Each of the nodes has a wireless interface to communicate with each other. These networks are fully distributed, and can work at any place without the help of any fixed infrastructure or access points or base stations. Routing is one of the core problems of networking for delivering data from one node to the other. Wireless ad-hoc networks are also called Mobile ad-hoc multi hop networks without fixed topology or central control. This is because MANETs can be characterized as having a dynamic, multi hop, potentially rapid changing topology. The aim of such networks is to provide communication capabilities to areas with limited or no existing communication infrastructures. A MANET is usually formed by mobile nodes using wireless communications. It uses a peer-to-peer multi hop routing instead of a immobile network infrastructure to provide network connectivity. Several multi hop routing protocols have been proposed for MANET. The most popular routing protocols are AODV (Adhoc On Demand Distance Vector), DSR (Dynamic Source Routing) and DSDV (Destination Sequence Distance Vector) etc.,

Security has become a primary concern in order to provide protected communication between mobile nodes in a hostile environment and the ultimate goal of the security solutions for MANETs is to provide security services such as Confidentiality, Integrity, Non repudiation and Authentication, Authorization and Anonymity.

Challenges in Mobile Ad-Hoc Networks:

Ad-hoc networks have to suffer many challenges at the time of routing. Dynamically changing topology and no centralized infrastructure are the biggest challenges in the designing of an Ad-hoc network. The position of the nodes in an Ad-hoc network continuously varies due to rapid change of network topology. Another challenge in MANET is limited bandwidth. If we compare it to the wired network then wireless network has less and more varying bandwidth. So, bandwidth efficiency is also a major concern in ad-hoc network routing protocol designing because sometimes data has to be transmitted within real time constraints. Limited power supply is the biggest challenge of an ad-hoc network so if we want to increase the network lifetime (duration of time when the first node of the network runs out of energy) as well the node lifetime then we must have an energy efficient protocol. So

Corresponding Author: M. Vijay Anand, Professor, Department of Computer Science and Engineering, Aksheyaa College of Engineering, India.
E-mail: mvijay200304@yahoo.co.in

Australian Journal of Basic and Applied Sciences, 9(10) Special 2015, Pages: 31-38

an ad-hoc routing protocol must meet all these challenges to give the average performance in every case. The main challenges in mobile ad-hoc networks are as follows:

- Limited Power Supply
- Dynamically Changing Topology
- Limited Bandwidth
- Security
- Mobility-induced route changes
- Mobility-induced packet losses
- Battery constraints

An Overview of Routing Protocols:

Destination Sequence Distance Vector (DSDV):

The first MANET algorithm that we implement as part of this work is called Destination Sequence Distance Vector (DSDV) routing algorithm. It is a proactive routing algorithm. The DSDV algorithm is a Distance Vector (DV) based routing algorithm designed for use in MANETs, which are defined as the cooperative engagement of a collection of Mobile Hosts without the required intervention of any centralized Access Point (AP).

Disadvantages:

(i)DSDV requires a regular update of its routing tables.
(ii)Battery power is less
(iii)It uses small amount of bandwidth even when the network is idle.
(iv)DSDV is not suitable for highly dynamic or large scale networks

Dynamic Source routing:

(DSR)is a routing protocol for wireless mesh networks. It is similar to AODV in that it forms a route on-demand when a transmitting node requests one. However, it uses source routing instead of relying on the routing table at each intermediate device. Determining source routes requires accumulating the address of each device between the source and destination during route discovery. The accumulated path information is cached by nodes processing the route discovery packets. The learned paths are used to route packets. To accomplish source routing, the routed packets contain the address of each device the packet will traverse. This may result in high overhead for long paths or large addresses, like IPv6. To avoid using source routing, DSR optionally defines a flow id option that allows packets to be forwarded on a hop-by-hop basis.

Disadvantages:

(i)Packet header size grows with route length due to source routing
(ii)Route request packet may potentially reach all nodes in the network
(iii) Route requests may collide at the targeted node
(iv)Every node needs to turn on its receiver all the time
(v)Increased contention if too many route replies come back
(vi)An intermediate node may send Route Reply using a stale cached route, thus polluting other nodes' caches.

Ad hoc On Demand Distance Vector (AODV):

The Ad hoc On Demand Distance Vector (AODV) routing algorithm is a routing protocol designed for ad hoc mobile networks. AODV is capable of both unicast and multicast routing. It is an on demand algorithm, meaning that it builds routes between nodes only as desired by source nodes. It maintains these routes as long as they are needed by the sources. AODV uses sequence numbers to ensure the freshness of routes. It is loop-free, self-starting, and scales to large numbers of mobile nodes.

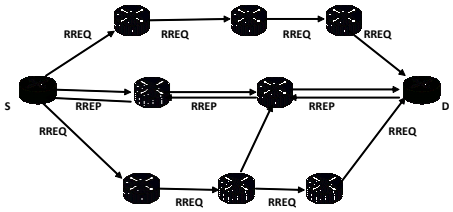

Fig. 1: Aodv Routing.

AODV builds routes using a route request / route reply query cycle. When a source node desires a route to a destination for which it does not already have a route, it broadcasts a route request (RREQ) packet across the network. Nodes receiving this packet update their information for the source node and set up backwards pointers to the source node in the route tables. In addition to the source node's IP address, current sequence number, and broadcast ID, the RREQ also contains the most recent sequence number for the destination of which the source node is aware. A node receiving the RREQ may send a route reply (RREP) if it is either the destination or if it has a route to the destination with corresponding sequence number greater than or equal to that contained in the RREQ. If this is the case, it unicast a RREP back to the source. Otherwise, it rebroadcasts the RREQ. Nodes keep track of the RREQ's source IP address and broadcast ID. If they receive a RREQ which they have already processed, they discard the RREQ and do not forward it.

Australian Journal of Basic and Applied Sciences, 9(10) Special 2015, Pages: 31-38

As the RREP propagates back to the source, nodes set up forward pointers to the destination. Once the source node receives the RREP, it may begin to forward data packets to the destination. If the source later receives a RREP containing a greater sequence number or contains the same sequence number with a smaller hop count, it may update its routing information for that destination and begin using the better route.

As long as the route remains active, it will continue to be maintained. A route is considered active as long as there are data packets periodically travelling from the source to the destination along that path. Once the source stops sending data packets, the links will time out and eventually be deleted from the intermediate node routing tables. If a link break occurs while the route is active, the node upstream of the break propagates a route error (RERR) message to the source node to inform it of the now unreachable destination(s). After receiving the RERR, if the source node still desires the route, it can reinitiate route discovery.

Advantages:

(i)The main advantage of this protocol is that routes are established on demand and destination sequence numbers are used to find the latest route to destination.

(ii)The connection setup delay is less.

Attacks in Adhoc Networks:

There are different types of attacks in Adhoc networks they are:

- Flooding attack
- Wormhole attack
- Black hole attack

Flooding attack:

Flooding attack can be launched by flooding the network with fake RREQs or data packets leading to the congestion of the network and reduces the probability of data transmission of the trusted nodes.

Wormhole attack:

The wormhole attack is quite severe, and consists in recording traffic from one region of the network and replaying it in a different region. For launching a wormhole attack, an adversary connects two distant points in the network using a direct low-latency communication link called as the wormhole link. The wormhole link can be established by a variety of means, e.g., by using an Ethernet cable, a long-range wireless transmission, or an optical link. Once the wormhole link is established, the adversary captures wireless transmissions on one end, sends them through the wormhole link and replays them at the other end.

The severity of the wormhole attack comes from the fact that it is difficult to detect, and is effective even in a network where confidentiality, integrity, authentication, and non-repudiation (via encryption, digesting, and digital signature) are preserved.

Black hole attack:

A Black hole is a malicious node that falsely replies for route requests without having an active route to the destination and exploits the routing protocol to advertise itself as having a shortest route to destination. By advertising the shortest route, source station starts sending data through the black hole node and it become the active element in the route.

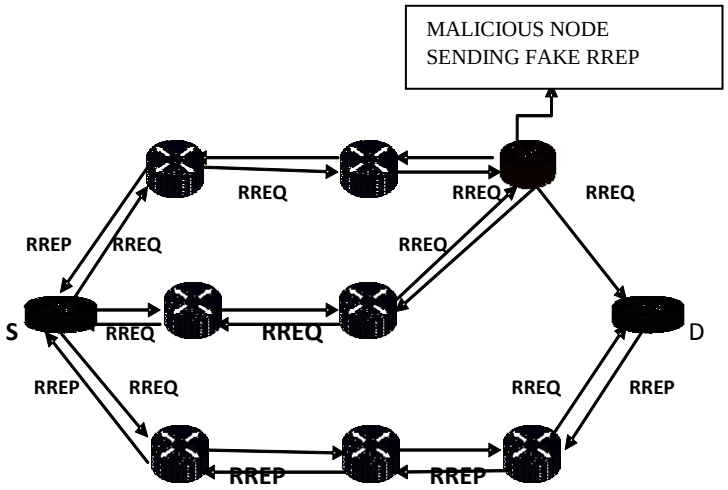

Fig. 2: Detecting Blackhole Attack.

Working Principle of Abc:

A new swarm intelligence algorithm, ABC (Artificial Bee Colony) is motivated by the deeds of honey bees. Since it was proposed by Karaboga , many extensions have been made to improve it Karaboga et al.compared the performance of ABC with that of some other popular meta heuristic optimization algorithms, such as particle swarm optimization (PSO), genetic algorithms (GAs), and differential evolution (DE). The results showed that it has a comparable performance with other algorithms. There are three agents in ABC algorithm,(i) scout bee (ii) onlooker bee (iii) employed bee.

Scouts:

It discovers new route from their launching node to their destination node. It starts from the hive in search a food source randomly keeping on this exploration process until they are tired. When they return back to the hive they convey to the foragers information about the odor of the food, its direction and the distance with respect to the hive by performing dance.

Employed bees:

Each employed bees is assigned to one of the food source. If the new food source has more nectar, the employed bees will replace the current food source with it. The employed bees whose food source has been abandoned becomes a scout bee, and carries out a random search to find a new food source after all employed bees complete the searching process, they share the information about the nectar amount and the position of food sources with onlooker bees by doing waggle dance.

Onlooker bees:

Onlooker bees watch the dance and select a food source based on its nectar amount. It does not participate in the route establishment.

Related Work:

[1]" A Bee-Hive Optimization Approach to Improve the Network Lifetime in Wireless Sensor Networks**"** S. Bhuvaneshwari et.al / International Journal on Computer Science and Engineering (IJCSE) Vol. 5 No. 05 May 2013. This paper is about Bee Hive Optimization (BHO) approach for increasing the lifetime of wireless sensor network. [2] **"**A Comprehensive review of Artificial Bee Colony Algorithm" Kamalam Balasubramani*/International Journal of Computers & Technology Volume 5, No. 1, May -June, 2013, ISSN 2277-3061. This paper is to provide a detailed study and research of ABC algorithm. [3] "Thwarting Attacks on ZigBee – Removal of the KillerBee Stinger" Bj¨orn Stelte and Gabi Dreo Rodosek/ISBN 978-3-901882-53-1, 9th CNSM and Workshops, 2013 IFIP. This paper is about the analysis of KillerBee framework and two relevant attack mechanisms. These attacks can be found by the newly proposed anomaly-based IDS technique.[4]"Comparative Analysis of Bee-Ant Colony Optimized Routing(BACOR) with Existing Routing Protocols for Scalable Mobile AdHoc Networks (MANETs) based on Pause Time", S. Kanimozhi Suguna, Dr.S.Uma Maheswari, IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.4, April 2012. In this paper based on swarm intelligence a new approach for an on demand ad-hoc routing algorithm is proposed. [5] "Identification and Removal of Black Hole Attack for Secure Communication in MANETs" Himani Yadav and Rakesh Kumar, ***I***nternational ***J***ournal of ***C***omputer ***S***cience and ***T***elecommunications [Volume 3, Issue 9, September 2012] This paper is about identification and removal of blackhole attack using modified ZRP protocol.[6] "BeeID: Intrusion Detection in AODV-based MANETs Using Artificial Bee Colony and Negative Selection Algorithms" Fatemeh Barani and Mahdi Abadi, http://www.isecure-journal.org, January 2012.This paper proposes a new intrusion detection technique using artificial bee colony algorithm and mitigating a wormhole attack. [7]"The Predicted Energy Efficient Bee-inspired Routing(PEEBR) Improvement and Performance Evaluation", Imane M. A. Fahrnv, Hesham A. Hefny, Laila Nassef,The 8th International Conference on Informatics and Systems (INFOS2012) - 14-16 May. This paper proposes a predict the amount of energy that will be consumed by all the nodes along each of the potential routing paths between a certain source node and a destination node using two types of bee agent. [8] "NISR: A Nature Inspired Scalable Routing Protocol for Mobile Ad Hoc Networks" Sajjad Jahanbakhsh Gudakahriz , Shahram Jamali , Esmaeel Zeinali, IJCSET | May 2011 | Vol 1, Issue 4,178-182. This paper proposes a new scalable routing protocol NISR which is inspired by nature. [9] "Bee-Inspired Routing Protocols for Mobile Ad hoc Network (MANET)", Deepika Chaudhary, Journal of Emerging Technologies In Web Intelligence, VOL. 2, NO. 2, MAY 2010. This paper provides a high light on energy efficient algorithm for routing in Manets BeeAdHoc. [10] "DPRAODV: A Dynamic learning system against black hole attack in aodv based MANET" Payal N. Raj, Prashant B. Swadas, IJCSI International Journal of Computer Science Issues, Vol. 2, 2009. This paper is about a new technique for security a DPRAODV (Detection, Prevention and Reactive AODV) to prevent security threats of black hole by notifying other nodes in the network of the incident.[11] "A Cross-layer Design for Bee-Inspired Routing Protocols in MANETs ",Alexandros Giagkos and Myra S. Wilson are with the Intelligent Robotics Group, Dept. of Computer Science, Aberystwyth University, Penglais, Aberystwyth, Ceredigion, Wales, UK, SY23 3DB. This paper is about adaptive nature inspired routing protocols of MANET**.** [12] "A Sense of Danger:

Dendritic Cells Inspired Artificial Immune System (AIS) for MANET Security" Nauman Mazhar, Muddassar Farooq GECCO'08, July 12–16, 2008, Atlanta, Georgia, USA. Copyright 2008 ACM978-1-60558-130-9/08/07. In this paper a new algorithm is proposed to detect misbehavior detection system called BeeAIS-DC. [13] "Vulnerability Analysis and Security Framework (BeeSec) for Nature Inspired MANET Routing Protocols", Nauman Mazhar, Muddassar Farooq, *GECCO'07,* July 7–11, 2007, London, England, United Kingdom. Copyright 2007 ACM 978-1-59593-697-4/07/0007. This is a survey paper which discuss about the role of malicious node in untrusted mobile adhoc network.[14]"BeeIP: Bee-Inspired Protocol for Routing in Mobile Ad-Hoc Networks", Alexandros Giagkos and Myra S. Wilson,2007. In this paper a Bee inspired routing protocol, BeeIP was used to achieve higher data delivery rates and less control overhead than DSDV, and slightly better results compared to AODV, initializing less route discovery processes. Our proposed protocol could ensures to provide a secured routing by mitigating the Black hole attack and increase the packet delivery ratio and reduced delay.

Proposed Work:

This paper proposes a new secure routing protocol called SABC-AODV. It uses the methodology of Artificial bee Colony algorithm and AODV protocol for secured routing. The SABC-AODV routing protocol isa bio-inspired reactive routing protocol. This protocol also ensures the security against black hole attack termed as **S**ecure **A**rtificial **B**ee **C**olony- **A**dhoc **O**n **D**emand **Di**stance Vector. To overcome the black hole attack in manet network it inherits cryptographic techniques.

Secured Artificial Bee Colony Algorithm(SABC):

Route Selection:

- Scouts broadcasts RREQ to all the employed bees.
- An employed bee sends RREP to scouts.
- The route will be selected based on the shortest path.

Random node selection:

- After all employed bees complete the searching process, they share the information about the nectar amount or the node is good or malicious node with onlooker bee by doing waggle dance and round dance.
- If the bee is performing a waggle dance that the node is trusted node.
- If the bee is doing a round dance that the corresponding node became a malicious node.
- Now onlooker bee watches the dance and selects a food source based on its dance performance.
- If the node is malicious create one dictator node and mobile node.
- The dictator node having group id and the id will be send to all the mobile nodes.
- Which mobile node is having the group id signature that the particular node can access the routing process.

Proposed Algorithm:

Initialize the nodes
Scout (S)
Employed Bees (E) - neighbor nodes
Onlooker Bees (O)
Distance (d)

Route Selection:

1. S broadcasts RREQ to all the e
2. E sends the RREP to S
3. If (d(RREP)==shortest)
4. The route is established
5. E discovering a new route from source to destination.

Random Node Selection:

After all E complete the search process, they share the information about the nectar amount or the node is good or malicious node with O by doing waggle dance and round dance.

6. If (dance==waggle)
Good node
Else
If (dance==round)
Malicious node / node having greatest sequence number is malicious
Now O watches the dance and selects a food source based on its dance performance.
7. If (node==malicious)
Create Dictator node
Dictator node: (it can share the key at initial time)
Normal node: (normal mobile node)

Dictator node initially sends the Group ID key to all then mobile node

8. If normal node received that ID then stores into memory
9. If node having GID
able to access the request
10. If not
Can't able to access the request
11. If node (x) wants to communicate with another node
Node x generates the hash code
Encrypting that code with private key of node x using RSA algorithm
sends to destination node
12. destination node can verify that encrypted message by using the public key and as well as group ID
if match
node y sending own code to source node x
if not match
ignore
13. if match code of node y

Australian Journal of Basic and Applied Sciences, 9(10) Special 2015, Pages: 31-38

transmit the data
14. if not match
ignore

Implementation:

The experiments for the evaluation of the scheme that validate the malicious node detection and packet delivery ratio of the proposed scheme against black hole nodes have been carried out using the network simulator NS-2 with VMware based back-Ground.

The simulations consist of 30 nodes evolving in a region of (1200m) during 100 seconds. Transmission range is set to 250 meters. Random waypoint movement model is used and maximum movement speed is 30m/s. Packets among the nodes are transmitted with constant bit rate (CBR) of one packet per second, and the size of each packet is 512 bytes. In these simulations, we used packet delivery ratio evaluation metrics. Performance comparison is made on the basis of this packet delivery ratio between existing AODV and proposed SABC-AODV. Finally the data packets are securely transmitted.

PDR is the ratio of the number of data packets received by the destination to the number of data packets sent by the source. This metric shows the reliability of data packet delivery.

Result:

The performance are analyzed based on Packet Delivery Ratio (PDR) and End to End delay.

Packet delivery ratio (PDR):

Ratio of number of packets received at the destination nodes to the number of packets sent from the source nodes is defined as Packet Delivery Ratio.
PDR=∑ Number of packet receive /∑ Number of packet send

End to End delay:

The average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted.
Delay=∑ (arrival time – sending time) / ∑ Number of connections

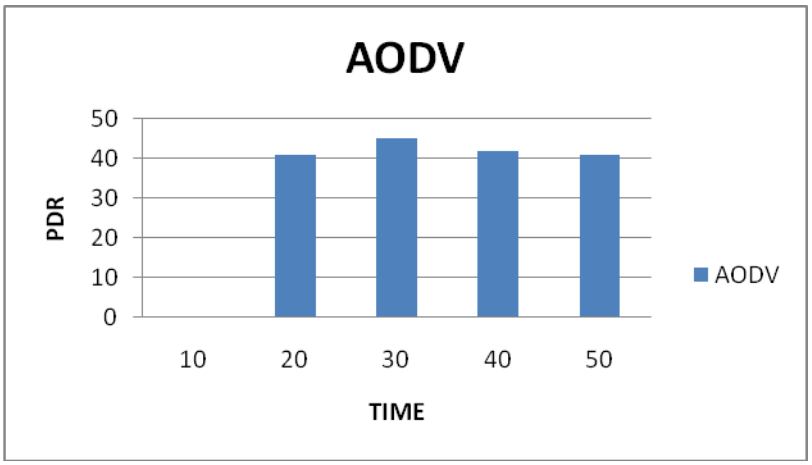

Fig. 3: Time Vs Packet delivery ratio.

Fig 3. shows results of normal AODV routing as time increases the packet delivery ratio decreases.

Fig 4. Shows the comparison results of packet delivery ratio for DSDV,AODV,SABC-AODV. As the number of nodes in the network increases PDR of AODV decreases due to increase in the number of intermediate nodes on a route. This is because the increase in number of intermediate nodes on an active route increases the probability of route failure. From the result it is found that the SABC-AODV protocol has improved packet delivery ratio when compared to other protocols.

Table 1: Time Vs Packet delivery ratio.

TIME (sec)	DSDV (Packets)	AODV (Packets)	SABC-AODV (Packets)
0	0	0	0
10	41	41	42
20	45	45	45
30	42	42	46
40	41	41	50
50	0	0	0
60	41	41	42

Australian Journal of Basic and Applied Sciences, 9(10) Special 2015, Pages: 31-38

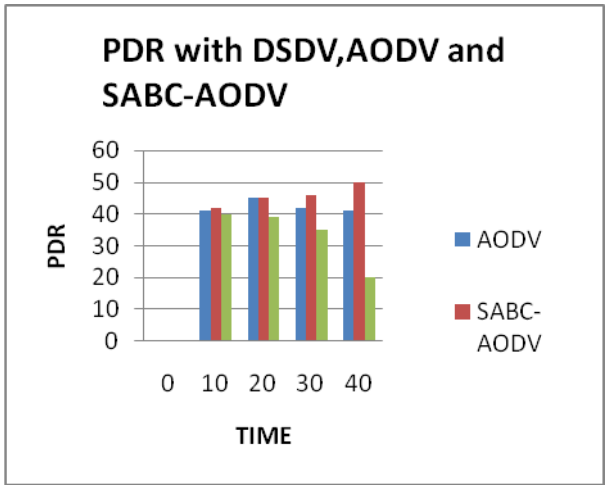

Fig. 4: Time Vs Packet delivery ratio.

Table 2: Node Vs End to End Delay.

NODE	DSDV (Time in sec)	AODV (Time in sec)	SABC-AODV (Time in sec)
0	140	140	110
10	190	120	180
20	170	80	120
30	120	240	80
40	90	110	110
50	100	140	50
60	140	140	110

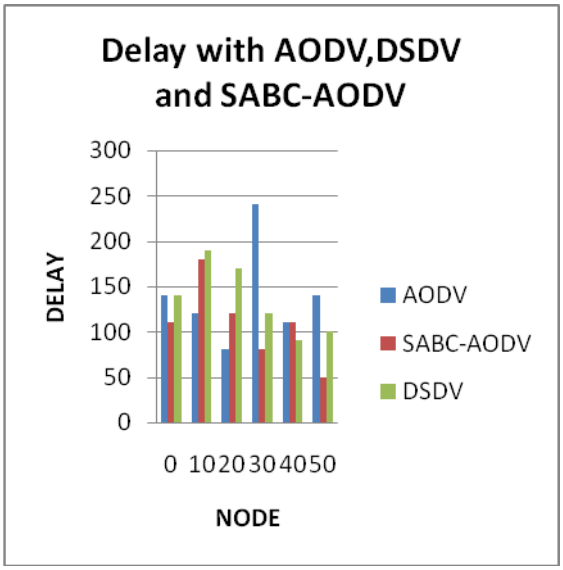

Fig. 5: Node Vs End to End Delay.

Fig.5. shows the comparison results of end to end delay for DSDV,AODV, SABC-AODV. The result describe that the proposed SABC-AODV protocol produces a minimum amount of delay compare to other routing protocols.

Conclusion:

In this paper SABC-AODV, an improved version of ABC and AODV routing protocol is proposed. This protocol not only mitigates the black hole attack using cryptographic algorithms. For secured routing but also ensures for the improved packet delivery ratio and reduced end to end delay when compared with other routing protocols.

In future this paper could be focused on secure data transmission and to detect/remove a black hole attacks using the DSR protocol with the bio inspired algorithm.

REFERENCES

Bhuvaneshwari, S., *et al*., 2013. "A Bee-Hive Optimization Approach to Improve the Network Lifetime in Wireless Sensor Networks"International

Journal on Computer Science and Engineering (IJCSE), 5(05).

Kamalam Balasubramani, 2013. "A Comprehensive review of Artificial Bee Colony Algorithm" /International Journal of Computers & Technology, 5(1): ISSN 2277-3061.

Bj¨orn Stelte and Gabi Dreo Rodosek, 2013. "Thwarting Attacks on ZigBee – Removal of the KillerBee Stinger" ISBN 978-3-901882-53-1, 9th CNSM and Workshops, IFIP.

Kanimozhi Suguna, S., Dr. S. Uma Maheswari, 2012. "Comparative Analysis of Bee-Ant Colony Optimized Routing(BACOR) with Existing Routing Protocols for Scalable Mobile AdHoc Networks (MANETs) based on Pause Time",IJCSNS International Journal of Computer Science and Network Security, 12(4).

Himani Yadav and Rakesh Kumar, 2012. "Identification and Removal of Black Hole Attack for Secure Communication in MANETs",*I*nternational *J*ournal of *C*omputer *S*cience and *T*elecommunications, 3(9).

Fatemeh Barani and Mahdi Abadi, 2012. "BeeID: Intrusion Detection in AODV-based MANETs Using Artificial Bee Colony and Negative SelectionAlgorithms", http://www.isecure-journal.org.

Imane, M.A. Fahrnv, Hesham A. Hefny, Laila Nassef, 2012. "The Predicted Energy Efficient Bee-inspired Routing(PEEBR) Improvement and Performance Evaluation", The 8th International Conference on Informatics and Systems (INFOS2012) - 14-16 May.

Sajjad Jahanbakhsh Gudakahriz, Shahram Jamali, Esmaeel Zeinali, 2011. "NISR: A Nature Inspired Scalable Routing Protocol for Mobile Ad Hoc Networks" IJCSET, 1(4): 178-182.

Deepika Chaudhary, 2010. "Bee-Inspired Routing Protocols for Mobile Ad Hoc Network (Manet)", Journal Of Emerging Technologies In Web Intelligence, 2(2).

Payal N. Raj, Prashant B. Swadas, 2009. "DPRAODV: A Dyanamic learning system against blackhole attack in aodv based MANET", IJCSI International Journal of Computer Science Issues, 2.

Alexandros Giagkos and Myra S. Wilson, "A Cross-layer Design for Bee-Inspired Routing Protocols in MANETs" ,Penglais, Aberystwyth, Ceredigion, Wales, UK, SY23 3DB.

Nauman Mazhar, Muddassar Farooq, 2008. "A Sense of Danger: Dendritic Cells Inspired Artificial Immune System (AIS) for MANET Security" GECCO'08, July 12–16, 2008, Atlanta, Georgia, USA. Copyright 2008 ACM978-1-60558-130-9/08/07.

Nauman Mazhar, Muddassar Farooq, 2007. "Vulnerability Analysis and Security Framework (BeeSec) for Nature Inspired MANET Routing Protocols", *GECCO'07,* July 7–11, 2007, London, England, United Kingdom.Copyright 2007 ACM 978-1-59593-697-4/07/0007.

Alexandros Giagkos and Myra S. Wilson, 2007. "BeeIP: Bee-Inspired Protocol for Routing in Mobile Ad-Hoc Networks.