**Available Online at www.ijcsmc.com**

**International Journal of Computer Science and Mobile Computing**

**A Monthly Journal of Computer Science and Information Technology**

**ISSN 2320–088X**

*IJCSMC, Vol. 3, Issue. 8, August 2014, pg.566 – 572*

**RESEARCH ARTICLE**

# ABC_AODV: ARTIFICIAL BEE COLONY BASED AODV ROUTING IN MANET

**Richa Kalucha[1], Deepak Goyal[2]**

[1]M.Tech Student, Vaish College of Engineering, MDU, Rohtak, Haryana (India)

[2]Associate Professor, Vaish College of Engineering, MDU, Rohtak, Haryana (India)

***Abstract- A MANET (Mobile Adhoc Network) is a collection of two or more devices that can communicate with another node that is immediately within their radio range or one that is outside their radio range. Due to flexibility of Ad-hoc networks nodes can join and leave a network easily. As wireless ad-hoc networks lack an infrastructure and are always unreliable, they are exposed to a lot of attacks. Black hole attack is one of the dangerous among them. In the Black Hole attack, a malicious node absorbs all data packets in itself, similar to a hole which sucks in everything. In this way, all packets in the network are dropped. A malicious node dropping all the traffic in the network makes use of the vulnerabilities of the route discovery packets of the on demand protocols, such as AODV. The goal of this work is to study the effects of Black hole attacks on reactive routing protocols i.e. Ad-Hoc on Demand Distance Vector (AODV) and New Ad-Hoc on Demand Distance Vector (nAODV).The proposed process uses the ABC algorithm to detect the Black Hole Attack. The Scout bees are used to search the black hole node. The Employed bee informs the network for the Black Hole node. And Onlooker bees take care of the Black Hole Node is not in the routing. ABC maximizes the lifetime of network and provides an effective multi-path data transmission in efficient manner.***

***Keywords: MANET, ABC, ACO, PSO***

## I. Introduction

A mobile ad hoc network is a self-organizing system of mobile nodes that in which wireless links communicates with no fixed infrastructure or centralized administration. Nodes in a MANET operate both as hosts and routers to forward packets for each other in a multi-hop fashion. MANETs are suitable for applications such as military battlefield, emergency rescue, vehicular communications and mining operations. MANETs has many advantages over traditional networks i.e. reduced infrastructure costs and fault tolerance, as routing is performed individually by nodes using other intermediate network nodes to forward packets [1].In Ad-hoc networks ,nodes communicate with each other without an infrastructure, they provide the connectivity by forwarding packets over themselves. For this connectivity, nodes use some routing protocols such as AODV (Ad-hoc On-Demand Distance Vector), DSR (Dynamic Source Routing) and DSDV (Destination-Sequenced Distance-Vector. [2][3].

 

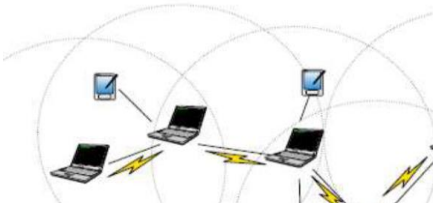

**Figure 1. MANET**

Security is an essential requirement in MANET. Due to the mobility and wireless nature of network malicious nodes can enter the network at any time; the security of the nodes needs to be considered. [4] As wireless ad-hoc networks lack an infrastructure, they are exposed to a lot of attacks

**MANETs characteristics**

1 Dynamic topology: Nodes can move freely with different speeds; this result in change of the network topology at unpredictable time. The nodes in the MANET establish routing dynamically among themselves as they travel around.

*2* Multi hop routing: When a node tries to send information to other nodes which is out of its communication range, the packet should be forwarded via one or more intermediate nodes.

3 Autonomous terminal: In MANET, each mobile node is an independent node, which could function as both a host and a router.

4 Light-weight terminals: In maximum cases, the nodes at MANET are mobile with less CPU capability, low power storage and small memory size. 5 Distributed operation: The control of the network is distributed among the nodes. The nodes in a MANET cooperate with each other and communicate among themselves and each node acts as a relay as needed, to implement specific functions such as routing and security.

*6* Shared Physical Medium**:** The wireless communication medium is accessible to any entity with the appropriate equipment and adequate resources. Accordingly, access to the channel cannot be restricted.[5]

## II. Black Hole Attack

Black hole attack is denial of service (DOS) attack in which malicious node send fake information by claiming that it has a shortest route to destination node .Therefore source nodes select this shortest path and go through this malicious node and results in misuse of data or data may be discarded [6]. Once the route is set up, it's up to the node whether to drop all the packet. This special node, which drops the data packet, is named as malicious nodes. Black hole has two main characteristics. First the node announces itself having a suitable route to a destination node and second one the node consumes the intercepted packets.

Once the attacker enters between the communicating nodes, it can do anything malicious with the packets. It can then choose to drop the packets. Security in mobile ad-hoc network is the most vital concern for basic functionality of a network [7]. Accessibility of network services, confidentiality and integrity of data can be achieved by assuring that security issues have been met. MANETs suffer from security attacks because they possess open medium, dynamic topology, lack of central administration. These factors lead to various security threats in mobile ad hoc networks [8]. Black hole Attacks are classified into two categories. In single blackhole attack there is only one malicious node within a zone [9]. Whereas in collaborative blackhole attack multiple nodes in a group act as malicious nodes [10].

 

## III. Artificial Bee Colony Algorithm

The Artificial Bee Colony (ABC) algorithm is proposed by Karaboga in 2005 for real-parameter optimization, which simulates the foraging behavior of a bee colony [11]. In ABC algorithm, each cycle consists of three steps : the employed bees are send onto their food sources and nectar amounts are evaluated; after sharing the nectar information of food sources, the onlookers bees select food source areas and evaluate the nectar amount of the food sources. The scout bees are sent randomly onto possible new food sources. At the initialization stage, a set of food sources is randomly selected by the bees and their nectar amounts are determined. At the first step of the cycle, these bees come into the hive and share the nectar information of the sources with the bees waiting on the dance area. A bee waiting on the dance area make decision to choose a food source is onlooker and the bee visited food source by herself just before is employed bee. After sharing their information with onlookers, every employed bee goes to the food source area visited by herself the previous cycle since that food source exists in her memory, and then chooses a new food source by means of visual information in the neighborhood of the one in her memory and evaluates its nectar amount. At the second step, an onlooker bee prefers a food source area depending on the nectar information distributed by the employed bees on the dance area. As the nectar amount of a food source increases, the probability of that food source chosen also increases. After arriving at the selected area, she chooses a new food source in the neighborhood of the one in the memory depending on visual information as in the case of employed bees.

At the third step of the cycle, scout bee determine new food source when the nectar of a food source is abandoned by the bees , and replaced with the abandoned one. In our work, at each cycle at most one scout goes outside for searching a new food source, and the number of employed and onlooker bees is selected to be equal to each other. These three steps are repeated through a predetermined number of cycles called Maximum Cycle Number (MCN) or until a termination criterion is satisfied.[12]

## IV. Proposed Work(nAODV)

The proposed process uses the ABC algorithm to detect the Black Hole Attack. The Scout bees are used to search the black hole node. The Employed bee inform the network for the Black Hole node.And Onlooker bees take care of the Black Hole Node is not in the routing.The process is explained in following steps:-

Step1**:** Select Source and Destination.

Step2: Generate an Artificial Bee at random nodes.

Step3: Transfer data from Source to Destination using AODV routing protocol.

Step4: Scout Bee search for Black Hole Node.

Step5: If Black Hole Node found then Employed Bee inform source to change path.

Step6: Onlooker Bee takes care that Black Hole Node not used in the routing.

## V. Result Validation

Here the detailed implementation of proposed approach is presented. Simulation is done using the network simulator tool NS2.In our Simulation there are 40 nodes placed randomly. Due to random dynamic topology, the source and the destination are also selected randomly.

 

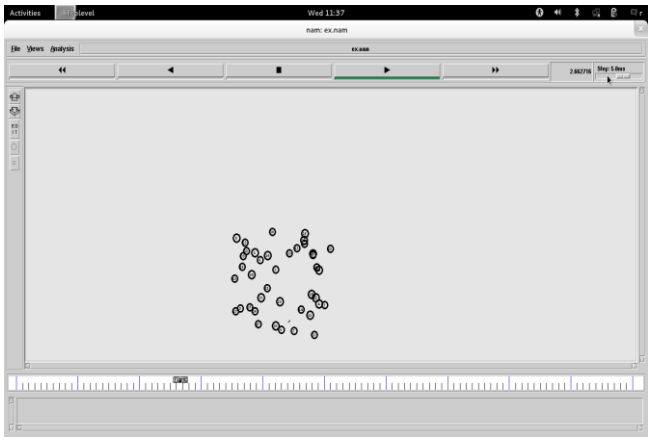

**Figure 2. PACKETS TRANSMISSION**

This fig shows the transmission of packets using selected path.

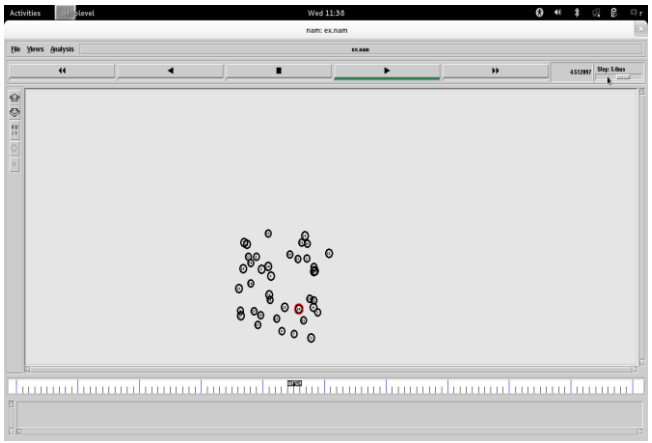

**Figure 3. Black Hole Node Detection**

This fig. shows Scout Bee searching for Black Hole Node.

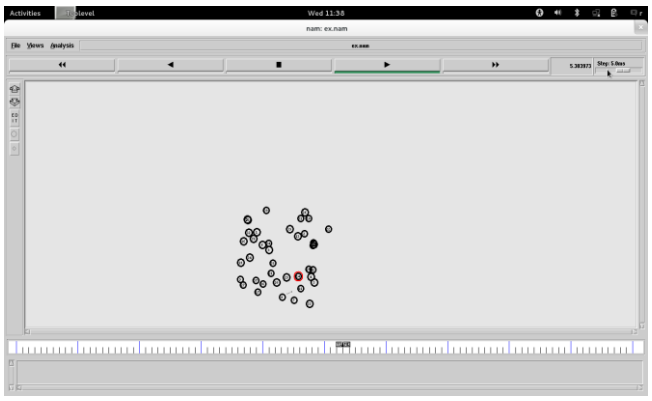

**Figure 4. PACKETS TRANSMIT TO ALTERNATE PATH**

This fig. shows if Black Hole Node found then Employed Bee inform source to change path and Onlooker Bee take care that Black Hole Node not used in the routing.

Our proposed system work more effectively than existing work by using some parameters. These parameters are help to show the better performance of our work than existing work.

 

Various parameters used for analysis are described below:

- Throughput: The amount of data transfer from source mode to destination in a specified amount of time i.e. average number of bits delivered per second(Kbps)

  Calculated as: Throughput =(Packet Size/(stopTime-startTime))*(8/1000)

- Packet Delivery Ratio: Packet delivery Fraction (PDF): It is the ratio of the amount of data packets delivered to the destination and total number of data packets sent by source.

  Calculated as: PDF=(Received Packets / Packets Sent)*100

- Average End to End Delay: The interval time between sending by the source node and receiving by the destination node, which includes the processing time and queuing time.

- Calculated as EED= (Time packet received - Time packet sent)

  Total number of packets received

**Table 1: Table showing performance analysis of existing ABC**

| No.Of Nodes | Generated packet | Received packet | Packet delivery ratio | End to End delay | Throughput |
|---|---|---|---|---|---|
| 10 | 244 | 212 | 86.8852 | 5.73753 | 242.19 |
| 20 | 284 | 257 | 90.493 | 8.75712 | 422.59 |
| 30 | 412 | 374 | 90.7767 | 5.94518 | 434.41 |
| 40 | 885 | 764 | 86.3277 | 2.91374 | 637.25 |

This table shows the performance analysis of existing AODV system on different number of nodes.

**Table 2: Table showing performance analysis of proposed ABC**

| NO. Of Nodes | Generated packets | Received packets | Packet delivery ratio | End to End delay | Through put |
|---|---|---|---|---|---|
| 10 | 2185 | 2104 | 96.2929 | 2.8244 | 1369.43 |
| 20 | 2367 | 2267 | 95.7752 | 3.03234 | 1336.28 |
| 30 | 2408 | 2271 | 94.6429 | 3.01579 | 1386.75 |
| 40 | 2822 | 2651 | 93.9405 | 2.60264 | 1543.36 |

This table shows the performance analysis of nAODV system on different number of nodes. This table depicts that value of all performance parameters shows fluctuating behavior with the increases number of nodes except average end- to- end delay.

 

Value of average end to end delay is decreases with the number of nodes. Value of Packet Delivery Ratio and throughput increases.

## VI. Graphs

These algorithms are implemented in NS2 Simulator. X-graph gives the results. X-graph gives the graphs for basic AODV and nAODV. When comparison between these graphs done then packet received of nAODV increases than the existing AODV and packet lost is reduced than existing AODV. In this results are shown for 10-40 nodes.In order to show the performance of the ABC algorithm more clearly, the graphical representations of the results in Table 1 are reproduced in Figs.5-7:-

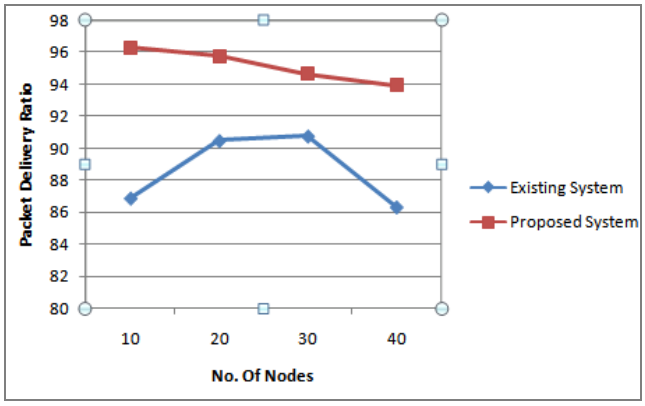


**Figure 5. Graph for the Packet Delivery Ratio of the 10-40 nodes between existing and proposed work**

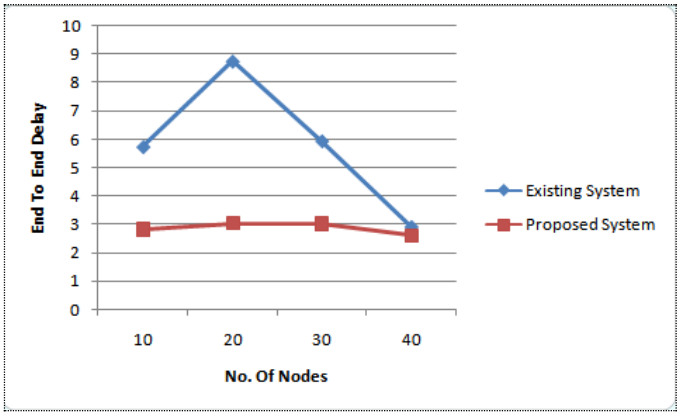


**Figure 6. Graph for the End To End Delay of the 10-40 nodes between existing and proposed work**.

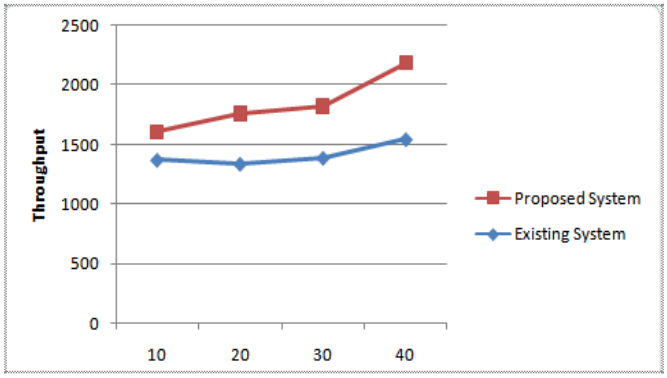


**Figure7. Graph for the Throughput of the 10-40 nodes between existing and proposed work**.

 

## VII. Conclusion and Future Work

In this paper we presented new protocol for MANET.As Security is an essential requirement in MANET. Due to the mobility and wireless nature of network malicious nodes can enter the network at any time; the security of the nodes needs to be considered.As wireless ad-hoc networks lack an infrastructure, they are exposed to a lot of attacks.Our proposed system work more effectively than existing work.The proposed process uses the ABC algorithm to detect the blackhole attack.In this Scout bees are used to search the black hole node. The Employed bees inform the network for the Black Hole node. And Onlooker bees take care of the Black Hole Node is not in the routing. Our study was concluded to evaluate the performance of artificial bee colony based algorithm in terms of Packet Delivery Ratio, end-to end delay and throughput the performance of ABC was better than existing process. The proposed work can be used to compare other swarm based techniques.It can be applied on dymo protocol.ABC algorithm can be applied on ZRP.

## References

[1] M. Zhang and P. H. J. Chong, "Performance Comparison of Flat and Cluster-Based Hierarchical Ad Hoc Routing with Entity and Group Mobility," in *Proc. of IEEE Communications Society conference on Wireless Communications & Networking*, Budapest, Hungary, 2009,pp. 2450-2455.

[2] M. G. Zapata and N. Asokan, "Securing Ad-Hoc Routing Protocols," *Proc. 2002 ACM Wksp. Wireless Sec.*, Sept. 2002, pp. 1–10.

[3] B. Wu *et al.*, "*A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks*," *Wireless/Mobile Network Security*, Springer, vol. 17, 2006.

[4] R. Akbani, T. Korkmaz, and G .V. S. Raju, "HEAP: *A packet authentication scheme for mobile ad hoc networks*," *Ad Hoc Networks*,vol. 6, no. 7, pp. 1134–1150, 2008.

[5] Aarti "*Study of MANET: Characteristics, Challenges, Application and Security Attacks*" International Journal of Advanced Research in Computer Science and Software Engineering May – 2013.

[6] Vinay P.Virada "*Securing And Preventing Aodv Routing Protocol From Black Hole Attack Using Counter Algorithm*" International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 8, October - 2012 ISSN: 2278-0181.

[7]. Loay Abusalah, Ashfaq Khokhar, and Mohsen Guizani, ―*A Survey of Secure Mobile Ad Hoc Routing Protocols*‖, IEEE Communications Surveys & Tutorials, Vol. 10, No. 4, Fourth Quarter 2008.

[8]. Dokurer, S.; Ert, Y.M.; and Acar, C.E., *Performance analysis of ad hoc networks under Black hole attacks*. Southeast Con, 2007, Proceedings IEEE, 148 – 153.

[9]. Latha Tamilselvan and Dr. V Sankaranarayanan, ―*Prevention of Black hole Attack in MANET*‖, The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, 0-7695-2842-2/07, 2007.

[10]. Santhosh Krishna B V, Mrs.Vallikannu A.L , ―*Detecting Malicious Nodes For Secure Routing in MANETS Using Reputation Based Mechanism*‖ International Journal of Scientific & Engineering Research, Vol. 1, Issue 3, ISSN 2229-5518, December-2010.

[11] D. Karaboga, *An Idea Based On Honey Bee Swarm for Numerical Optimization*, Technical Report TR06, Erciyes University, Engineering Faculty, Computer Engineering Department, 2005.

[12]Dervis Karaboga *, Bahriye Akay, "*A comparative study of Artificial Bee Colony algorithm*" Applied Mathematics and Computation 214 (2009) 108–132.

 