WALAILAK JOURNAL
http://wjst.wu.ac.th Minireview

# A Survey on Algorithms Based on Bee Swarms for Ad Hoc Networks

**Marjan KUCHAKI RAFSANJANI[*] and Hamideh FATEMIDOKHT**

*Department of Computer Science, Shahid Bahonar University of Kerman, Kerman, Iran*

**([*]Corresponding author's e-mail: kuchaki@uk.ac.ir)**

*Received: 1 December 2012, Revised: 20 January 2013, Accepted: 23 February 2013*

**Abstract**

Ad hoc networks are wireless networks with new architectures, which are formed in any environment that is needed, without a fixed infrastructure. Due to a lack of central management and fixed infrastructure, and the poor physical security of nodes, these networks are extremely vulnerable. As the usage and development of ad hoc networks increases, problems related to these networks are a popular research topic. Hence, efficient and effective algorithms, such as bee algorithms, were created, which were inspired by the foraging principles of honey bees. In this paper, we study algorithms based on bee swarms in ad hoc networks.

**Keywords:** Ad hoc networks, Bee swarm intelligence, routing, efficiency

## Introduction

Ad hoc networks are established, without using a fixed infrastructure or centralized administration, in any environment that needed. They are useful in many applications. In recent years, due to improved wireless technology, these networks have been widely used. Examples of applications of ad hoc networks can be found in areas where earthquakes or other natural disasters have destroyed communication infrastructures, and for emergency rescue and military operations. Some of the advantages of ad hoc networks are mobility, flexibility, scalability, the elimination of fixed infrastructure costs, and the reduction of power consumption [1]. Due to the characteristics of ad hoc networks, such as lack of infrastructure, resource limitation, node energy, etc [1], and the applications of them, problems related to these networks, such as routing security and efficiency, are significant topics. Swarm intelligence (SI) algorithms, such as bee algorithms, have shown to be a good and effective technique for ad hoc networks. SI is the collective behavior of autonomous agents that locally interact with each other. SI can be used in a number of applications. The bee algorithm is a swarm based meta-heuristic algorithm inspired by the foraging principles of honey bees in nature. When the bee hive searches for food, the queen bee sends scout bees in search of nectar sources. After completing their search, they return to the hive and report their information by performing a dance. After that, follower bees are sent to the best possible location of the food source, so that the food can be transported [2]. This paper is organized into 3 parts. In the first part, we describe bee behavior in nature. Then, we introduce protocols for ad hoc networks inspired by bee behavior; finally, we display the applications, advantages, and disadvantages of the discussed algorithms.

## Bees in nature

Bees are social and domestic insects that live together as colonies. They are divided into 3 kinds, the queen, drones, and workers, and carry out several assigned tasks, like brood tending, storing, retrieving and distributing honey and pollen, communication, and foraging [3].

**Queen bee**

The queen bee is generally the mother of all bees in the hive, and her main task is lay eggs. A healthy queen bee can lay 2,000 eggs a day and 175,000 - 200,000 eggs per year. She has small wings and does not have the ability to collect the nectar of flowers. Normally, she cannot survive more than 5 years.

**Drones**

The main task of drones is to fertilize the queen bee; they are the fathers of the colony. They have large heads and wings, have the ability to collect nectar and pollen, and survive for 24 days. Drones are grown in larger cells than worker bees, and are produced from unfertilized eggs.

**Workers**

Workers bees are female and constitute the majority of the population of the hive. They are not capable of being fertilized; however, in the absence of the queen in the hive, they can spawn. They have barbed stingers, with a length of about 1 millimeter. They live for 6 weeks during the summer and 4 - 9 months during the winter.

**Search for food in nature by honey bees**

A colony of honey bees can be distributed over large distances and various vectors to exploit food sources. The process of the food search begins with a scout bee that is sent to search for promising food sources. After completing their search, they return to the hive and report their information by performing a dance, which represents the percentage density of food over the area and the orientation of the search area. The next step in searching for food is sending follower bees to the best possible location of the food source, so they can transport the food. The foraging principles of honey bees in nature are [2]:

- To generate a population of scout bees.
- To send them to search neighborhood.
- To repeat till no results are found.
- To evaluate scout bee in searching areas.
- To select the best possible sites from scout bee areas.
- To select the scout bees with the best quality finds.
- To reassign the remaining bees to further scout searches.

**Protocols for ad hoc networks inspired by bee behavior**

In this part, we express some algorithms for ad hoc networks that have designs based on the foraging principles of honey bees in nature.

**BeeAdHoc**

Wedde and colleagues [4] have presented BeeAdHoc, which is a routing algorithm for mobile ad hoc networks inspired by the foraging principles of honey bees in nature. It is a reactive source routing algorithm for energy efficiency. It uses scouts and foragers for discover new routes and transport data from source to destination, respectively. When a route to a destination is needed, a forward scout is transmitted to all the neighbors of a node with an expanding time to live timer (TTL). The intermediate nodes that receive the scout append their addresses to the source route of the scout until it arrives at the destination. When the forward scout reaches the destination, the destination node creates a backward scout by reversing the source route, and sends it back to the source. Once the scout returns to its source node, it advertises the route to other foragers, and then the foragers, which are informed through the metaphor of dance, transport data to the destination node. The foragers collect the routing information of the network that is used to compute the dance number, which represents the quality of the path traversed.

**BeeSec**

Mazhar and Farooq [5] have introduced this framework; BeeSec is a secure version of BeeAdHoc that utilizes asymmetric cryptography based digital signatures. In BeeSec, scouts and foragers use digital

signatures that are computed with source address, destination address, packet ID, routing information, and so on. Also, the integrity of the source route is maintained, to ensure that malicious nodes are prevented from removing valid nodes on the route. Consequently, BeeSec prevents tampering and fabrication attacks in BeeAdHoc, and is able to successfully counter the attacks launched against the routing protocol; however, its extreme large processing and communication overheads make it inappropriate for deployment on battery constrained mobile nodes.

**BeeAIS**

Mazhar and Farooq [6] have presented BeeAIS, an Artificial Immune System (AIS) model for securing BeeAdHoc. It is based on self non-self discrimination, and uses negative selection for anomaly detection. BeeAIS first learns the system self in the learning phase, over a duration of 50 s, and then monitors the system for occurrences of non-self, associated with malicious activity. It uses 3 types of antigens, a scout antigen, and 2 forager type antigens. The scout antigen detects abnormal behavior in the forward and backward scouts, and the 2 forager antigens detect anomalies in the source route and routing information carried by a forager. Therefore, BeeAIS can detect previously unknown attacks. However, it has a mobility limitation, namely, when node mobility causes the system self to change; it is unable to learn the changing self, and therefore the average throughput of BeeAIS is low.

**BeeAIS-DC**

Mazhar and Farooq [7] have offered this framework; BeeAIS-DC is the third approach for securing BeeAdHoc, and uses danger theory concepts for detecting routing misbehavior. It uses dendritic cells (DCs) to provide the ability to adaptively learn the changing self, and overcomes the mobility limitation of BeeAIS. The use of a danger signal prevents the need for an initial learning phase at the system start up time. By sensing the presence/absence of danger in tissue, BeeAIS-DC is able to differentiate between self and non-self behavior. However, BeeAIS-DC utilizes scout antigens/detectors that only make it able to counter scout related attacks on BeeAdHoc.

**BeeIP**

Giagkos and Wilson [8] have introduced BeeIP, which is a bee inspired routing protocol for MANETs that uses cross-layering. This protocol uses three types of agents in the form of data packets: a scout for discovering new paths towards a given destination, a ask_scout for traveling back to the source, and a forager for transmitting packets to their destination. BeeIP uses local reliability levels to measure how good or bad a way between a pair of nodes for transmission. Global reliability levels indicate the link's quality as experienced during the last forager's flight, which is a summation of all the local reliability differences that the forager collects on its way back.

**iBeeAIS**

Mazhar and Farooq [9] have designed this security framework for BeeAdHoc. IBeeAIS is an integrated AIS security framework for misbehavior detection in BeeAdHoc. Its features enable dynamic learning of the system self and non-self, since in iBeeAIS, antigens in a tissue are sampled by DCs, and tissue context is classified as self or non-self. IBeeAIS uses activation of B-cells, which endure affinity maturation for a more focused response against suspected non-self antigens. Due to the integrated AIS detection process, iBeeAIS can learn the changing non-self through feedback from DCs. Therefore, iBeeAIS has good detection accuracy with low false alarm rates for scout and forager related attacks.

**Clustered artificial bee colony**

Santhiya and Arumugam [10] have offered Adaptive Bio-Inspired Clustered Routing for MANET. A cluster consists of linked nodes that work together, so that in many respects they can be viewed as a single system. In mobile ad hoc networks, clustering helps in maintaining a relatively stable effective topology. The ABC algorithm uses three kinds of bees: employed bees, onlooker bees and scout bees. In clustered ABC, within each cluster, employee bees publish the information. Each onlooker bee selects a source depending on the quality of the solution, produces a new source in a selected source site, and

exploits the better source with the information derived from the employee bees. This framework can be implemented for a real time environment.

**Bee life algorithm**

Bitam and Mellouk [11] have introduced this algorithm for routing optimization for vehicular ad hoc networks. The bee life algorithm starts with an initial random population in the search space. A bee population contains 1 queen, D drones and W workers. Each cycle of algorithm consists of 2 bee behaviors, reproduction and food foraging. In reproduction, after generation N broods by crossover and mutation, the fitness of the broods is evaluated. If the fittest brood is fitter than the queen, then it replaces the queen for the next population. Then, for forming next generation drones, D best bees are chosen among the D fittest following broods and drones of the current population. To ensure food foraging, W best bees are subsequently chosen among the W fittest remaining broods and workers of the current population. In food foraging behavior, the first search for a food source in W regions is performed by W workers. Then, the bees for each region for neighborhood searches are recruited. For each region, the fittest bees will be selected to form the next bee population, and the fitness of the new population is evaluated. After these 2 bee behaviors, if the stopping criterion is not satisfied, a new bee life cycle is performed; otherwise, the algorithm is ended.

**BeeSensor**

Saleem and colleagues [12] have proposed this protocol, which is an energy efficient and scalable routing protocol for wireless sensor networks. BeeSensor uses 4 types of agents: packers, scouts, foragers and swarms. The major task of packers is to receive and store data packets from the transport layer. Scouts explore new routes in the network to a sink node. Foragers are the main workers in BeeSensor; their major role is to transport data packets to the destination. Sometimes foragers need to be explicitly transported back to their source node; this need is served by a swarm agent. Phases of the BeeSensor protocol include scouting, foraging, swarming and routing loops, and path maintenance.

**Artificial Bee Colony (ABC)**

Ozturk and colleagues [13] have presented the ABC algorithm that is utilized for the dynamic deployment of wireless sensor networks. In this algorithm, the position and the amount of a food source indicate a possible solution and quality of the associated solution, respectively. The ABC algorithm includes 3 groups of bees: employed bees, onlookers and scouts. It starts with initial parameters, such as detection radius, size of area of interest, number of mobile sensors, colony size, maximum number of iterations, and limitations for scouts. Then, $m$ sensors are randomly deployed for each food source $x_i$ of employed bees, and the population evaluated. As long as the maximum number of iterations does not expire, a new solution $v_i$ in the neighborhood of $x_i$ for employed bees is produced and checked for staying in the bounds of the area, and then a greedy selection process between $x_i$ and $v_i$ is performed and probability values $P_i$ for solution $x_i$ calculated. After that, the new solution, $v_i$, for the onlooker bees from solutions $x_i$, is produced and a greedy selection process between $x_i$ and $v_i$ for the onlookers is performed; then the best solution achieved thus far is memorized and, eventually, the abandoned solution is determined. If it exists, it is replaced with a new randomly produced solution.

**Discussion on discussed algorithms**

The discussed algorithms in the previous part are presented in **Table 1**. In **Table 2**, we display the advantages and disadvantages of the algorithms.

**Table 1** Discussed algorithms and their applications.

| Algorithm | Application | Type of network |
|---|---|---|
| BeeAdHoc (2005) [4] | Energy efficient routing | Mobile ad hoc networks |
| BeeSec (2007) [5] | Security framework for routing | Mobile ad hoc networks |
| BeeAIS (2007) [6] | AIS security for routing | Mobile ad hoc networks |
| BeeAIS-DC (2008) [7] | DC inspired AIS security for routing | Mobile ad hoc networks |
| BeeIP (2010) [8] | Routing | Mobile ad hoc networks |
| iBeeAIS (2011) [9] | Hybrid AIS security for routing | Mobile ad hoc networks |
| Clustered artificial bee colony (2012) [10] | Clustered routing | Mobile ad hoc networks |
| Bee life algorithm (2013) [11] | QOS-multicast routing | Vehicular ad hoc networks |
| BeeSensor (2012) [12] | Energy efficient and scalable routing | Wireless sensor networks |
| Artificial bee colony (2012) [13] | Dynamic deployment | Wireless sensor networks |

**Table 2** Advantages and disadvantages of the algorithms.

| Algorithm | Advantages | Disadvantages |
|---|---|---|
| BeeAdHoc (2005) [4] | Small energy expenditure, small detection delay | Vulnerable to Byzantine attacks |
| BeeSec (2007) [5] | Counter the different type of threats, Small energy expenditure and small detection delay | Very large processing and communication overheads |
| BeeAIS (2007) [6] | Anomaly detection using the negative selection, Small energy expenditure and small detection delay | Mobility limitation |
| BeeAIS-DC (2008) [7] | Overcomes the limitation in BeeAIS | Detect only scout related attacks |
| BeeIP (2010) [8] | Uses cross-layering, delivering more data packet successfully, initializes less route discovery processes than AODV | Does not support multiple paths for each transmission |
| iBeeAIS (2011) [9] | High detection accuracy, small detection delay, approximately zero control overhead of the ADS framework, small processing overhead and detects scout and forager related attacks | ---------- |
| Clustered artificial bee colony (2012) [10] | Effective optimal route discovery, enhanced scalability, QOS guarantees and minimal end-to-end delay | ---------- |
| Bee life algorithm (2013) [11] | Proves efficiency and performance of solution quality and complexity | Uses a low number of nodes |
| BeeSensor (2012) [12] | Least energy consumption, scalable and efficient | Validates on not very large-scale sensor networks |
| artificial bee colony (2012) [13] | Good performance and increases the coverage area | Includes only mobile sensors and not stationary ones |

## Conclusions

Ad hoc networks are sets of nodes that are connected via wireless links without using a fixed infrastructure or centralized administration. Due to applications to ad hoc networks, the efficiency of these networks is a significant topic. In this paper, we have reviewed some algorithms that are inspired by the foraging principles of bees in nature. In **Tables 1** and **2** we displayed the applications, advantages, and disadvantages of the algorithms. From these tables, we can conclude that the algorithms simulating bee behavior are effective and efficient algorithms for ad hoc networks.

## References

[1] R Hekmat. *Ad-Hoc Networks: Fundamental Properties and Network Topologies.* Springer, 2006.
[2] SK Dhurandher, S Misra, P Pruthi, S Singhal and S Aggarwal. Using bee algorithm for peer-to-peer file searching in mobile ad hoc networks. *J. Net. Comput. Appl.* 2011; **31**, 1498-508.
[3] D Karaboga and B Akay. A survey: Algorithms simulating bee swarm intelligence. *J. Artif. Intell. Rev.* 2009; **31**, 61-85.
[4] HF Wedde, M Farooq, T Pannenbaecker and B Vogel. BeeAdHoc: An energy efficient routing algorithm for mobile ad hoc networks inspired by bee behavior. *In:* Proceedings of the ACM Genetic and Evolutionary Computation Conference, Washington DC, USA, 2005, p. 153-60.
[5] N Mazhar and M Farooq. Vulnerability analysis and security framework (BeeSec) for nature inspired MANET routing protocols. *In:* Proceedings of the ACM Genetic and Evolutionary Computation Conference, London, UK, 2007, p. 102-9.
[6] N Mazhar and M Farooq. BeeAIS: Artificial immune system security for nature inspired, MANET routing protocol, Beeadhoc. *In:* Proceedings of the International Conferences on Artificial Immune Systems, LNCS 4628, Springer-Verlag, 2007, p. 370-81.
[7] N Mazhar and M Farooq. A sense of danger: Dendritic cells inspired artificial immune system (AIS) for MANET security. *In:* Proceedings of the ACM Genetic and Evolutionary Computation Conference, Atlanta, Georgia, USA, 2008.
[8] A Giagkos and MS Wilson. BeeIP: Bee-inspired protocol for routing in mobile ad hoc networks. *In:* Proceedings of the 11th International Conference on Simulation of Adaptive Behavior, Paris, 2010, p. 263-72.
[9] N Mazhar and M Farooq. A hybrid artificial immune system (AIS) model for power aware secure Mobile Ad Hoc Networks (MANETs) routing protocols. *J. Appl. Soft. Comput.* 2011; **11**, 5695-714.
[10] KG Santhiya and N Arumugam. A novel adaptive bio-inspired clustered routing for MANET. *J. Proc. Eng.* 2012; **30**, 711-7.
[11] S Bitam and A Mellouk. Bee life-based multi constraints multicast routing optimization for vehicular ad hoc networks. *J. Net. Comput. Appl.* 2013; **36**, 981-91.
[12] M Saleem, I Ullah and M Farooq. BeeSensor: An energy-efficient and scalable routing protocol for wireless sensor networks. *J. Info. Sci,* 2012; **200**, 38-56.
[13] C Ozturk, D Karaboga and B Gorkemli. Artificial bee colony algorithm for dynamic deployment of wireless sensor networks. *Turk. J. Electr. Eng. Comput. Sci.* 2012; **20**, 255-62.