IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 14, 2017, accepted September 26, 2017, date of publication October 12, 2017,
date of current version November 28, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2762472

A Survey of Ant Colony Optimization Based Routing Protocols for Mobile Ad Hoc Networks

HANG ZHANG, XI WANG, PARISA MEMARMOSHREFI, AND DIETER HOGREFE
Institute of Computer Science, Georg-August-University of Goettingen, Goettingen 37077, Germany
Corresponding author: Hang Zhang (hang.zhang@cs.uni-goettingen.de)

ABSTRACT Developing highly efficient routing protocols for Mobile Ad hoc NETworks (MANETs) is a challenging task. In order to fulfill multiple routing requirements, such as low packet delay, high packet delivery rate, and effective adaptation to network topology changes with low control overhead, and so on, new ways to approximate solutions to the known NP-hard optimization problem of routing in MANETs have to be investigated. Swarm intelligence (SI)-inspired algorithms have attracted a lot of attention, because they can offer possible optimized solutions ensuring high robustness, flexibility, and low cost. Moreover, they can solve large-scale sophisticated problems without a centralized control entity. A successful example in the SI field is the ant colony optimization (ACO) meta-heuristic. It presents a common framework for approximating solutions to NP-hard optimization problems. ACO has been successfully applied to balance the various routing related requirements in dynamic MANETs. This paper presents a comprehensive survey and comparison of various ACO-based routing protocols in MANETs. The main contributions of this survey include: 1) introducing the ACO principles as applied in routing protocols for MANETs; 2) classifying ACO-based routing approaches reviewed in this paper into five main categories; 3) surveying and comparing the selected routing protocols from the perspective of design and simulation parameters; and 4) discussing open issues and future possible design directions of ACO-based routing protocols.

INDEX TERMS ACO, ACO based routing, swarm intelligence, MANETs.

I. INTRODUCTION

Unlike from wired networks, Mobile Ad hoc NETworks (MANETs) are infrastructureless networks which consist of wireless mobile devices. Since these mobile devices can join and leave the network freely, the network topology can change very frequently. Due to the lack of infrastructure, devices in such networks need to cooperate with each other and work in a self-organized manner through wireless channels. Therefore, developing proper routing protocols for MANETs is a challenging task. Since the 1990s, many state-of-the-art routing protocols have been proposed for MANETs, such as Destination-Sequenced Distance Vector routing (DSDV) [1], Ad hoc On-demand Distance Vector (AODV) routing [2] and Dynamic Source Routing (DSR) protocol [3]. However, these routing protocols proposed long time ago focus on solving basic routing requirements and can hardly fulfill the various new requirements of MANETs' routing nowadays. Besides the basic routing requirements, new routing protocols designed for MANETs are supposed to work in a self-organized manner and provide low packet delay, high packet delivery rate and effective adaptation to network topology changes with low control overhead. Since biologists and nature scientists have found that activities in many biological systems such as ant colonies and bee colonies are based on simple rules and don't rely on any centralized control structure [4], many meta-heuristics inspired by the biological systems have been introduced by scientists in the past two decades. Beni and Wang [5] introduced the expression of Swarm Intelligence (SI) in their research of cellular robotic systems in 1993. The concept of SI is employed in work on Artificial Intelligence (AI). SI is a computational intelligence technique which is based on the collective behavior of decentralized, self-organized systems [6]. A typical SI system is made up of a group of simple agents which interact locally with each other and with the environment surrounding them [7]. Agents in an SI system follow simple rules and act without the control of any centralized entities. However, the social interactions between such agents may generate enormous benefits and often lead to a smart global behavior. As shown in Fig. 1, Kordon pointed out in [6] the main advantages of applying SI. SI takes the full advantage of the swarm, therefore, it's able

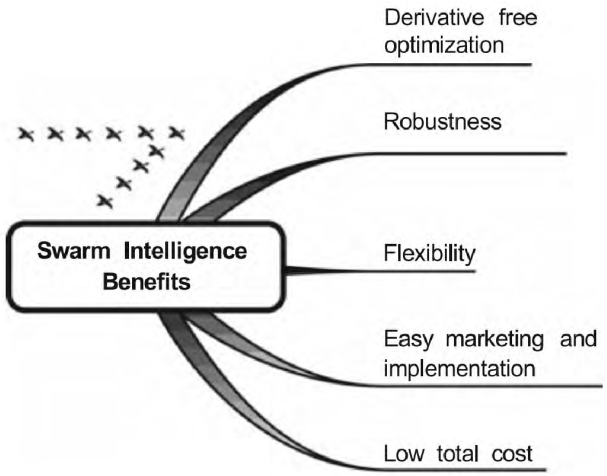


FIGURE 1. Swarm Intelligence Benefits [6].

to provide optimized solutions, which ensure high robustness, flexibility and low cost, for large-scale sophisticated problems without a centralized control entity [6]. Stochastic Diffusion Search (SDS) [8], Particle Swarm Optimization (PSO) [9] and Ant Colony Optimization (ACO) [10] are some well-known meta-heuristics in SI field. ACO algorithms have attracted a lot of attention as a design paradigm for new approaches that maintain and optimize routing in self-organizing and dynamic ad hoc networks.

In our previous work [11], we have surveyed the location aware ACO routing protocol for MANETs, especially for Vehicle Ad hoc NETworks (VANETs). However, this is only one special category of ACO based routing protocols in MANETs. In this comparative analytical paper we extend our research scope and give an overview of various ACO based routing protocols for MANETs applied in five main categories. Comparisons of the existing protocols are presented in terms of protocol design and simulation parameters. For a better understanding of how ACO algorithms are practically applied in these routing protocols, we select some particular ACO related parameters, for example, the ant types, the pheromone reinforcement and evaporation factors.

The rest of this paper is organized as follows. In Section II the background of the ACO meta-heuristic is presented. Based on five main categories, various of ACO based routing algorithms are presented in Section III. A comparative analysis of the studied protocols in each category is presented in the form of different tables which display design related parameters in Section IV. Another comparative analysis of all reviewed protocols that focuses on simulation parameters and a general discussion of the open issues and possible future directions in the field of ACO based routing protocols are given in Section V. Finally, Section VI concludes the work.

II. THE BACKGROUND OF ACO

A. ANTS IN NATURE

Ants are ubiquitous insects which began to diversify 100 million years ago [12]. Now, more than 8800 known species of ants [13] still exist across the globe. In nature, ants are well known type of social insects. The size of an ant colony can vary from a few dozen to millions. In an ant colony, there are usually different castes. ''Workers'' are the most common ants which could be found in any colony. They are small sterile females that take over most of the work in the colony: foraging food, maintaining and expanding the nest, taking care of the queen and brood, and so on. ''Queens'' are the fertile females which are the founders of all colonies. The main task of a queen is to lay eggs. ''Drones'' are the only male ants in a colony and they only survive during the mating season. In some special ant colonies, there could also be other castes, such as ''soldiers'', which are larger and stronger than typical ''workers''. As the name indicates, ''soldiers'' protect their colony from predators. Although each caste in the colony has different tasks, all castes work together collectively to ensure the colony's survival [14], [15]. It's well known that a single ant is not very bright, but ants in a colony can finish remarkable tasks, such as dealing with floods. In [16] researchers have found that ants can link their body to built self-assemblages. For instance, in order to beat floods, fire ants are able to use their bodies to built rafts in short time. Mlot *et al.* [17] have also measured the strength and speed by which ant rafts are built in another study. It shows that thousands of ants can rearrange themselves to build a stable raft within 200 seconds, and ants can use a force of 400 times their own weight to keep the raft. Observations in [17] and [18] show that ants can react to their environment quickly and survive under adverse environmental conditions.

Different from human, ants rarely use sound or sight to exchange information with each other. Instead, ants produce volatile chemical substance which is known as pheromone. Pheromone is the key component of ant's communication. While moving around, ants lay pheromone through their glands along their path and ants use their antennas to detect the pheromone in the surrounding area. There are different types of pheromone perfumes which represent different chemical words that the whole ant colony understands. Ants react differently corresponding to the type of pheromone detected. For instance, in order to alarm nest-mates, some species of ants create alarm pheromones by using their poison glands [19]. This kind of alarm pheromone includes two components: formic acid and n-undecane. By detecting the alarm pheromone, worker ants either escape fast or go towards the danger, in case that they are the defenders of the colony. Another well-known type of pheromone is the trail pheromone. This kind of pheromone is used by ants while foraging. An ant foraging for food leaves its nest and chooses randomly a direction to move on, as far as it doesn't find a pheromone trail. If it finds one, it has a high probability to follow the trail. No matter which decision it has made, it deposits pheromone over its route. Once it find the food, it returns to the nest and reinforces its trail. Other ants which detect its trail will follow the trail with great probability and lay more pheromone over it. This is a positive feedback loop system since the higher the trail's pheromone, the higher the

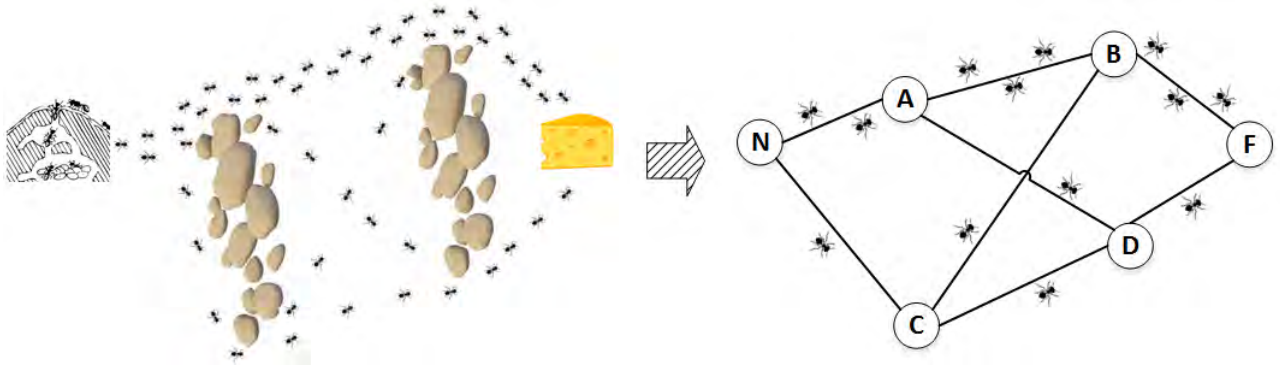


FIGURE 2. A representation example while applying ACO meta-heuristic.

probability of an ant to follow the trail. When the food is exhausted, no more pheromone is deposit on the trail and the pheromone begins to evaporate over the time. This negative feedback behavior supports ants to adapt to the dynamic environment [20].

B. FROM NATURE TO ARTIFICIAL ANTS

Assemblages of ants take on similar functions like those existing in the human societies, but ants don't rely on any central control to provide these functions. Therefore, understanding how the systems of ant colonies work has long been an attractive subject of study. In the 1980s, Moyson and Manderick [21] studied self-organization behavior among ants. Goss *et al.* proposed the initial idea of ant colony optimization algorithms based on their study of the collective behavior of ants in [22]. In this work, the author designed a simple, yet brilliant experiment: the double bridge experiment. In this experiment, an ant nest and a food source are connected by a double bridge which consists of two bridges with different lengths. The experiment's results indicate that the short path attracts more ants to follow, if both short and long paths are given to the ants in the same time. Moreover, the short path attracts much less ants, if it is given after the long path is followed by the ants for a while. This indicates that the pheromone evaporation rate controls the trade-off between path-exploration and path-exploitation [20]. Based on the foraging behavior of ants, Dorigo [10] initially proposed the Ant Colony Optimization (ACO) algorithm, the first ant-inspired algorithm aimed to find an optimal path in a graph, in his dissertation and published it in 1992. In cooperation with Gambardella, Dorigo proposed the Ant Colony System (ACS) in 1997 [23]. Since then, research in this area was followed by many other scientists and many popular variations of ACO algorithms were proposed. Bullnheimer textitet al. [24] proposed the Rank-based Ant System in 1997. Maniezzo [25] introduced ANTS: exact and approximate nondeterministic tree-search procedures for the quadratic assignment problem in 1999. Stützle and Hoos [26] invented the MAX-MIN Ant System (MMAS) in 2000. Blum and Dorigo [27] proposed a hyper-cube framework for ant colony optimization (HC-ACO) in 2004.

ACO is one of the research directions in applied SI and we will introduce more of its details in the following section.

C. THE ANT COLONY OPTIMIZATION ALGORITHM

The Ant Colony Optimization (ACO) meta-heuristic which belongs to the SI field is inspired by the foraging behavior of ants in nature. In ACO meta-heuristic, artificial ants work together to find good solutions for difficult combinatorial optimization problems [28]. Recall in the nature case, an ant deposits pheromone on its traveled path to mark its trail and inform other ants. When subsequent ants find a trail, they have a high probability to follow it. Once a subsequent ant follows the trail, it lays down new pheromone over the path. As consequence, the pheromone of the trail is reinforced and it might attract more ants to follow. Therefore, the pheromone represents the indirect information exchange between the individual ants.

In order to apply ACO algorithm to solve an optimization problem in real life, the considered problem firstly needs to be represented in a way that each potential solution of the problem is a path in a construction graph [29]. For example, the problem of how to find the optimal path between the ants' nest and the food source can be represented in a construction graph as shown in Fig. 2. Thus, the initial problem is mapped to the new problem on how to find the optimal path between node N and node F.

After finding the construction graph, the constraints of the problem should be defined. In this case, the constraint is that ants can only move on the arcs which connect the nodes in Fig. 2.

Each arc in Fig. 2 can have associated pheromone trails and a heuristic value [28]. The pheromone trail represents a long-term memory about the ant search process. For each destination there is a separate pheromone trail assigned to the arc. In contrast, there is only one heuristic value at each arc and it is a prior knowledge about the problem instance or run-time information provided by other sources. In many cases, this value is the cost of adding the arc to solution under construction.

In this example, the solution construction is straightforward: every ant in this construction graph starts at a single node N and aims for the same destination node F. Ants follow a probability decision rule to exploit the network. This probability rule is a function of local pheromone trails and heuristic information, and it can also be related to the ant's private memory and the problem constraints [28]. The common applied probability rule [28] can be represented as equations (II.1) and (II.2):

$$P_{ij}(t) = \begin{cases} \dfrac{\left[\tau_{ij}(t)\right]^{\alpha} \cdot \left[\eta_{ij}\right]^{\beta}}{\sum_{l \in N_i} \left[\tau_{il(t)}\right]^{\alpha} \cdot \left[\eta_{il}\right]^{\beta}}, & \text{if } j \in N_i \quad \text{(II.1)} \\ 0, & \text{if } j \notin N_i \quad \text{(II.2)} \end{cases}$$

where $P_{ij}(t)$ is the probability of an ant to move from node i to node j at the t^{th} iteration step or time slot; N_i is the set of current neighboring nodes of node i; $\tau_{ij}(t)$ is the pheromone intensity on the arc between node i and j at t^{th} iteration step or time slot; η_{ij} is the heuristic information of the arc between node i and j and it's usually a non-increasing function of moving cost from node i to node j; α and β are weight parameters which control the relative impact of pheromone intensity $\tau_{ij}(t)$ versus heuristic information η_{ij}. If α value is high, then the pheromone intensity has a strong impact to ants. In this case ants are more biased to follow the path which is chosen popularly by previous ants. This further leads to a situation in which all ants would eventually construct the same path. If α value is low, then the ACO algorithm is close to a stochastic greedy algorithm. When $\alpha = 0$, ants select the next hop node only based on the heuristic information, eg. cost. In contrast, ants are attracted only by the pheromone intensity when $\beta = 0$. Equation (II.2) shows that ants can only move to the neighboring nodes.

Once an ant leaves node N, it moves to one of its neighbor nodes according to equation (II.1). Every artificial ant has a memory space which is used for storing path related information, such as the nodes visited in its trip. An artificial ant moves hop by hop until it reaches the destination node F or another terminal condition is satisfied, for example the maximum travel hop count of the ant is reached. If the ant finds the destination node F, it retraces exactly the same path backward to the start point, node N. Once an ant has constructed a solution, or while building a solution, the ant evaluates the solution or partial solution to decide the amount of pheromone updates.

The update of pheromone trail can be either increased or decreased. The pheromone update amount assigned to an arc is calculated based on the quality of a solution in which this arc is involved, and the pheromone evaporation rate, as shown in equation (II.3). The first parameter is evaluated by an ant as an amount which is inversely proportional to the cost of the path. The pheromone evaporation rate is predefined and it allows ants to forget the outdated solutions and to explore new solutions. A simple form for the pheromone update procedure which is adapted from book [28] can be described as below:

$$\tau_{ij} \leftarrow (1 - \rho) \cdot \tau_{ij} + \sum_{k=1}^{m} \Delta\tau_{ij}^{k} \quad \text{(II.3)}$$

where τ_{ij} is the pheromone value laid by ants on the arc of node i and node j, namely $arc(i, j)$; $\rho \in (0, 1]$ is the pheromone evaporation rate; m is the number of ants; $\Delta\tau_{ij}^{k}$ is the amount of pheromone reinforcement deposited by the k^{th} ant for the $arc(i, j)$:

$$\Delta\tau_{ij}^{k} = \begin{cases} Q/C^{k}, & \text{if } arc(i,j) \in P^{k} \quad \text{(II.4)} \\ 0, & \text{if } arc(i,j) \notin P^{k} \quad \text{(II.5)} \end{cases}$$

where Q is a positive application-specific constant; P^k is the set of arcs chosen by the k^{th} ant in its path; C^k is the overall cost function of the current path which is constructed by the k^{th} ant. For example, C^k can be the length of the path constructed by k^{th} ant or the delay of finding a destination, or the available bandwidth of the link or the energy consumption of each node along the way and so on. Which parameters should be considered in the cost function depends on the concrete application.

There are many other variations of ACO, the concrete equations applied for path search and pheromone update could be varied from the ones previously introduced in this section. However, the ACO algorithm can be generally described as the interplay of three procedures [28], as shown in Fig. 3. ConstructAntsSolutions is the procedure in which a colony of ants concurrently find the solutions in the construction graph. UpdatePheromones is the process in which ants modify the pheromone trails. DaemonActions is an optional procedure which is designed for implementing centralized actions. These three procedures conduct many researchers to design their own protocols.

```
procedure ACOMetaheuristic
  ScheduleActivities
    ConstructAntsSolutions
    UpdatePheromones
    DaemonActions          % optional
  end-ScheduleActivities
end-procedure
```

FIGURE 3. The ACO meta-heuristic in pseudo-code [28].

The main merit of the ACO meta-heuristic is that it presents a common framework for approximating solutions to NP-hard optimization problems. Due to the dynamic nature of ACO's connectivity, ACO is able to continuously adapt to network changes in real time [20]. Moreover, the artificial ants can find multiple solutions simultaneously for the considered problem [28]. Therefore, it makes ACO specially applicable to dynamic problems, such as routing in telecommunication

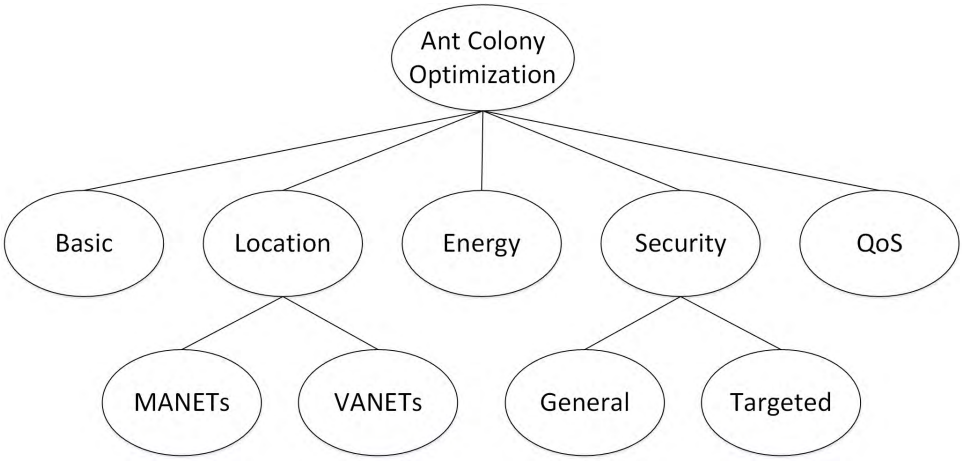


FIGURE 4. Types of ACO based routing protocols in MANETs.

networks. Since the middle 1990s, the number of applications based on the ACO algorithms has bloomed. Until now, ACO algorithms have already been applied to solve routing problems in MANETs and WSNs with better scalability than other approaches. In the following section, we will have a close look at the existing ACO applications in MANETs.

III. REVIEW OF ACO BASED ROUTING PROTOCOLS IN MANETs

Since the end of 1990s, ant inspired algorithms have been applied to solve routing problems in network communications. By now, a great number of such approaches exists. In this section, we will describe some well-known ACO based routing protocols for MANETs. We include not only the initial designs which aim at providing optimal routes, but also different approaches which consider special issues, such as Quality of Service (QoS), energy reserves, location information and security during the route setup process. In order to give a better overview, we categorize them into five main directions based on the design purposes of the protocols. Fig. 4 shows our categorization scheme in detail.

A. BASIC ACO ROUTING PROTOCOLS

Initially, the optimization property of ACO algorithms has attracted much attention. Inspired by it, researchers have been motivated to apply ACO algorithms to find optimized routes for network communications. There are many approaches that belong to this category. In this subsection we introduce the most famous ones in chronological order.

1) AntNet

Di Caro and Dorigo [30] have proposed AntNet, which is the first representative ACO-based algorithm for solving the problem of internet routing. In AntNet, each node proactively sends out Forward ANTs (FANTs) to discover a path to a randomly chosen destination node. Once FANTs reach the destination, Backward ANTs (BANTs) are sent back to the source node following the reverse path. BANTs update the local models of the network status and the local routing table at each intermediate node. The performance of AntNet is evaluated in three different wired network scenarios.

2) ARA

Another representative ACO-based routing protocol for MANETs, ARA was proposed by Günes *et al.* [31]. ARA is an on-demand routing algorithm, which is based on a simple ant colony optimization meta-heuristic algorithm. The whole routing algorithm consists of three phases: a route discovery phase, a route maintenance and a route failure handling. The route discovery phase in ARA is designed in a similar way to AntNet. FANTs and BANTs are used in the route discovery phase. FANTs are broadcasted by the sender. Duplicate FANTs are identified by their sequence numbers and are deleted by intermediate nodes. Once FANTs reach their destination nodes, BANTs are created and sent back to the source nodes. Different from AntNet [30], ARA uses data packets to maintain the route to avoid the overhead caused by using periodic ants. If a node recognizes a link failure, it first sets the pheromone value of this link to zero to deactivate it. Then it searches for an alternative link. If this fails, it informs its neighbors. This process is repeated until an alternative route has been found or the source node receives a route error message. In the latter case, the source node will initiate a new route discovery phase if there are still packets to be sent.

3) PERA

Baras and Mehta [32] have proposed PERA, a proactive routing protocol. PERA uses ant-like agents to discover the network topology and maintain routes in dynamic networks such as MANETs. PERA uses three kinds of ants: regular FANTs, uniform FANTs and BANTs. Regular and uniform FANTs are sent out proactively. These ants explore and reinforce available routes in the network. Uniform FANTs are routed in a different way than regular FANTs. Instead of using the routing table at each node, uniform FANTs choose the next hop node with uniform probability. Uniform FANTs help

avoid that previously discovered paths become overloaded. BANTs are used to adjust the routing tables and statistic tables at each node, according to the information gathered by FANTs. The authors have compared PERA with AODV [2]. The results indicate that PERA has lower delay in all cases. However, the throughput of PERA at the higher speed is slightly less than AODV and the goodput of PERA is lower than AODV in high mobility scenarios.

4) AntHocNet

Di Caro *et al.* [33] have presented a hybrid multi-path routing algorithm, AntHocNet. In AntHocNet there are 6 different kinds of ants: Proactive FANTs (PFANTs), Proactive BANTs (PBANTs), Reactive FANTs (RFANTs), Reactive BANTs (RBANTs), RePair FANTs (RPFANTs) and RePair BANTs (RPBANTs). In the reactive route setup process, if a source node has no routing information about the requested destination node, it broadcasts RFANTs. Otherwise, it unicasts. When this RFANT reaches the destination, a RBANT is sent back to the source. Along its journey, the RBANT collects quality information about each link in the path and updates the pheromone table at each intermediate node. Once the first route is constructed, AntHocNet starts the proactive route maintenance process. Here, source nodes send out PFANTs to their destination nodes. PFANTs consider both regular and virtual pheromone for choosing the next hop node at each intermediate node. Once a PFANT reaches the destination node, it is converted to a PBANT. PBANTs update the regular pheromone table on their way back to the source node. In case of a link failure, RPFANTs and RPBANTs are used to handle the problem. The authors have implemented the protocol in QualNet [34] and investigated its performance using various simulations and comparing the results to AODV [2].

5) PACONET

Osagie *et al.* [35] have proposed an improved ACO algorithm for routing called PACONET. In PACONET, a source node reactively broadcasts FANTs in a restricted manner to explore the network. Each FANT records the total time it has traveled and maintains a list of all visited nodes. At each intermediate node the FANT updates the pheromone value. Once a FANT arrives at the destination, a corresponding BANT is generated. The BANT uses the list of visited nodes recorded by the FANT to travel back to the source node. Along the way, the BANT also updates the pheromone value in the reverse direction. Different from the AntNet, PACONET let both FANTs and BANTs update the pheromone. The performance of PACONET has been compared with AODV [2].The results show that PACONET has less end to end delay and routing control overhead than AODV, but the packet delivery ratio is nearly the same.

6) ACO-AHR

Yu *et al.* [36] have proposed a hybrid routing algorithm ACO-AHR, which includes reactive routing setup and proactive routing probe and maintenance. There are two kinds of agents: ant agents and service agents. The ant agent are FANTs and BANTs as in other ACO based routing algorithms. In the reactive routing setup process, a source node broadcasts FANTs. Along the trip, each FANT records all the nodes it has visited in order to avoid cycles in the path. Each BANT carries all the information collected by the corresponding FANT. It calculates the delay from one intermediate node to the destination node. Once a BANT ant reaches the source node, a service agent is created. The service agent updates the routing table at intermediate nodes by using the information gathered by the BANT. In the proactive routing maintenance process, proactive FANTs are sent out while the data session is ongoing. The proactive FANTs are normally unicasted, but they could be broadcasted with a small probability. In the latter case, the FANTs may be able to find new paths.

7) HOPENT

HOPENT is proposed by Wang *et al.* [37]. It is based on the zone routing framework, combined with an ACO algorithm. HOPENT performs local proactive route discovery within a node's neighborhood and reactive communication between neighborhoods. HOPENT is simulated on GlomoSim [38] and the authors have compared HOPNET with several famous routing protocols, such as AODV [2], AntHocNet [33], and ZRP [39]. The results indicate that HOPNET is highly scalable for large networks in comparison with AntHocNet [33]. Moreover, the author also varied the zone radius in the experiments and results indicate that the selection of the zone radius has considerable effect on the performance.

8) ANT-E

Sethi and Udgata [40] have proposed an ACO-based on-demand routing protocol Ant-E. Ant-E uses Blocking Expanding Ring Search (Blocking-ERS) [41] to limit overhead and controls local retransmission to improve the Packet Delivery Ratio (PDR). The authors compared Ant-E with AODV [2] and DSR [3]. The results show that Ant-E performs better.

9) SUMMARY

In this section we have introduced some of the representative protocols which were proposed in the early stage of ACO based routing protocols. The first ACO based routing protocol, AntNet, proposed in 1998, gave a good example of how to apply the ACO algorithm in communication networks. In the following ten years, many subsequent researchers proposed various ACO based routing protocols for MANETs based on this idea. Protocols in this category aimed for finding the optimal routes in dynamically changing networks and their performance indicated that ACO is a promissing solution for routing problems in MANETs. This further encouraged researchers to design novel ACO based routing protocols which consider other issues, such as Quality of Service (QoS), energy consumption and so on.

B. QoS AWARE ACO ROUTING PROTOCOLS

QoS has always been a focus of attention in mobile ad hoc networks. It is a challenging problem when transmitting packets via multiple paths in a dynamic network. At the same time, the pheromone concept from ant colony algorithms also inspires many authors to use QoS parameters for selecting routes.

1) ARAMA

ARAMA is an early proactive routing algorithm proposed by Hussein and Saadawi [42]. The FANTs in ARAMA gather both local and global path information, which could be the Quality of Service (QoS) parameters such as the remaining battery energy, delay, numbers of hops, etc. ARAMA defines a local normalized link index which is a good measure for overall path information. Once the FANT reaches the destination, the path grade is calculated based on this path index. A BANT follows the reverse path to the source node and updates the pheromone table at each hop.

2) SAMP-DSR

SAMP-DSR is proposed by Khosrowshahi-Asl *et al.* [43], which aims to solve the shortcomings of both ACO and DSR [3] algorithms. In SAMP-DSR, each node can operate in two modes, called ''local mode''İ and ''global mode''. Depending on the rate of network topology change, nodes switch between the two modes, in order to help the ants converge efficiently.

3) QAMR

QAMR is a QoS-enabled ant colony based multipath routing protocol for MANETs which is proposed by Krishna *et al.* [44]. It selects paths based on Next Hop Availability (NHA) and the path preference probability. The NHA is defined as the availability of nodes and links for routing on a path, considering both mobility and the energy factors. In order to find the best path that satisfying the QoS constraints, QAMR uses a path preference probability which measures different parameters such as delay, bandwidth and hop count. However, there are many extra control messages for estimating the quality of outgoing links.

4) QoRA

Al-Ani and Seitz [45] have introduced a QoS Routing protocol for multi-rate ad hoc networks based on Ant colony optimization (QoRA). In order to reduce the overhead when collecting information from multiple paths and to avoid congestion during data transmission, this paper uses the Simple Network Management Protocol (SNMP) [46] to estimate QoS parameters locally. The proposed mechanism consists of two components: the QoRA entity and the SNMP entity. The QoRA entity runs on every node to identify a suitable route that meets the specified QoS requirements, while the SNMP entity collects detailed information about the characteristics of the outgoing links such as bandwidth, delay and packet loss. More specifically, the QoRA entity consists of five components: the neighbor table, the routing table, the ant Management, the decision engine and the QoS manager. while the two tables are common components of a routing protocols, the other three components are specially designed for QoRA. The ant management is responsible for generating FANTs, BANTs and EANTs, all of which contain specific information necessary to provide QoS-aware routing and to identify pheromone deposits. The QoRA decision engine is a vital part which decides which of the different ants are to be sent and which updates the neighbor and routing table. The QoS manager acts as a command generator and notification receiver application. It also calculates QoS parameters locally based on communication with the SNMP entity. QoRA consists of five phases regarding route discovery and route maintenance. The first phase is the forward phase. The source node broadcasts a FANT to the network to find the best route to the destination. Before forwarding the packets, each intermediate node checks the FANTStack to avoid loops and whether the given QoS requirements are satisfied. In the packet forwarding phase, intermediate nodes read the flow information and randomly forward the packets based on a probability roulette-wheel selection scheme [47] using the data in its routing table. The Backward phase starts after the destination node receives FANTs. The destination node calculates the residual QoS values and sends a BANT back to its neighbors. The BANT collects route quality information, refreshes the routing table, updates the pheromone and computes the QoS threshold. The Monitoring phase is mainly used for avoiding congestion problems by monitoring decreasing transmitting speeds. For each flow, QoRA communicate with the SNMP entity to calculate QoS parameters locally. If the required QoS is not satisfied in a certain period time (Monitoring Window), the affected node broadcasts an EANT to inform the previous nodes about the congestion problem. When a node detects the loss of a link to a neighboring node, it deletes the information about this neighbor node from the neighbor table and updates the route table by finding an alternative path using EANTs. The QoRA protocol does not require either exchanging additional control packets or synchronizing nodes with the help of the SNMP entity. It computes QoS parameters locally to reduce overhead. The computation of QoS parameters is all loaded to the SNMP entity which allows the QoRA protocol to reduce end-to-end delay. Although it is clear that the QoRA entity requires less overhead, the communication between the QoRA entity and SNMP entities consumes more energy and bandwidth.

5) SUMMARY

In this section we discuss five representative protocols which focus on QoS fulfillment. QoS has always been a vital task for data transmission in MANETs. The approaches focus mainly on the parameters: link stability and hop count. Other common QoS related improvements are a reduction in overhead produced by control messages and the ability to eschew the requirement of time synchronization. Many other QoS parameters such as link delay, remaining battery energy,

end to end reliability and bandwidth are treated as pheromone reinforce factors in above protocols.

C. ENERGY AWARE ACO ROUTING PROTOCOLS

In general, energy efficiency is one of the key parameters which should be considered while designing new routing protocols for wireless mobile networks and especially for Wireless Sensor Networks (WSNs). As shown before in section III-A, some of the proposed ACO based routing protocols for MANETs have used nodes' power reserves as a criterion in QoS computation. However, many conventional routing protocols suffer from sudden deaths of nodes in the network, because packets are always transmitted through the shortest paths. Therefore, nodes which participate in the shortest paths consume more power than other nodes. Network load imbalance leads to a reduction of network's lifetime. This problem recently has received more attention and many energy-efficient protocols which aim to extend network lifetime are proposed. The ACO-EEAODR [48] and EAAR [49] protocols are two earlier attempts in this direction.

1) ACO-EEAODR

Woungang *et al.* [48] have improved the energy-efficient ad hoc on-demand routing protocol by embedding an ACO algorithm into it, calling the result ACO-EEAODR. This protocol considers both the remaining battery power and the length of the path, while selecting the most energy-efficient path. There is a tradeoff between the two parameters. Due to the priority of energy efficiency in this protocol, the weight of the first criterion is set to 0.7. Moreover, the updates of pheromone values in each node are also based on the remaining battery power. In other words, an ant prefers hopping to a node with higher battery power rather than following the shortest path.

2) EAAR

An Energy-Aware Ant based Routing (EAAR) protocol is proposed by *Misra et al.* [49]. In order to increase the battery life of a node, it considers both multi-path transmission and power consumption in forwarding a packet. The residual battery capacity is also considered in the proposed algorithm. The Maximum of the minimum Residual Battery energy (MRB) of a route and the hop count are used to update the pheromone in the routing table during the route discovery phase. The results show that EAAR has the minimal energy consumption in the overall network and a low packets loss rate compared to AntHocNet [33]. However, the energy consumption per packet and the delivery rate are not as superior as the previous mentioned two parameters in high mobility scenarios. This is probably because EAAR needs more time to select the best route for data transmission.

3) AntHocMMP

Vijayalakshmi *et al.* [50] have proposed a robust energy efficient ACO routing algorithm named AntHocMMP, which uses ant agents to find optimal paths based on the Max-Min-Path (MMP) approach. The proposed algorithm first selects a set of relative paths from the source node to the destination by using the MMP algorithm. In the second phase FANTs are broadcast on all relative paths. While traversing along the relative paths, FANTs update the pheromone values at each intermediate node, to find the shortest and most robust path. Additional, AntHocMMP uses an adaptive re-transmission approach to detect link failure and select new relative paths. However, in the first phase the MMP algorithm has already traversed all the possible energy efficient paths from the source to destination and the pheromone deposits do not affect the selection of relative paths. Therefore, in this approach, the ACO algorithm is not used for finding possible paths, but for selecting the optimal path. This two procedure based approach is different from conventional ACO based routing approaches.

4) ACECR

Zhou *et al.* [51] have introduced the ant colony based energy control routing protocol (ACECR) for MANETs. Different from the EAAR [49] which considers only the residual battery power of nodes, ACECR takes both the average energy and the minimum energy of a path into account, in order to select a path with more residual energy when considered from a global view. During the route discovery phase BANTs update not only the pheromone table by calculating the minimum and summing up of the nodes' residual energy values, but also the average energy of a path and hop count. Fig. 5 shows an example of the pheromone table, which is a two-dimensional array. The row and the column denote destination nodes and neighboring nodes of node C, respectively. The value $P_{B,A}$ in the pheromone table is the amount of pheromone on the path from node C to the destination A via neighbor node B. The pheromone amount $P_{B,A}$ represents how good the path is to transmit a data packet. The authors have tested the protocol's performance with three different mobility models, namely the random walk mobility model, the random waypoint mobility model and reference point group mobility. All the simulation results show that ACECR has better performance than EAAR with respect to the data packet delivery ratio, routing load ratio, energy consumption of nodes and average end-to-end delay.

5) HYBRID ACO

Recently, Prabaharan and Ponnusamy [52] have proposed a hybrid ACO routing protocol that emphasizes the security and energy efficiency. We abbreviate this protocol as Hybrid ACO from here on. In contrast to the conventional ACO routing protocols, this hybrid ACO routing approach selects the next hop node by using Simulated Annealing (SA). SA is a probabilistic approach which has a low probability of sinking into local optima. In the initial phase of the transmission, each link in the network is given a trust value as the initial pheromone value. Once the source node needs to discover a new route, it sends out FANTs. Before moving to the next hop, each FANT shortlists 5 neighboring nodes

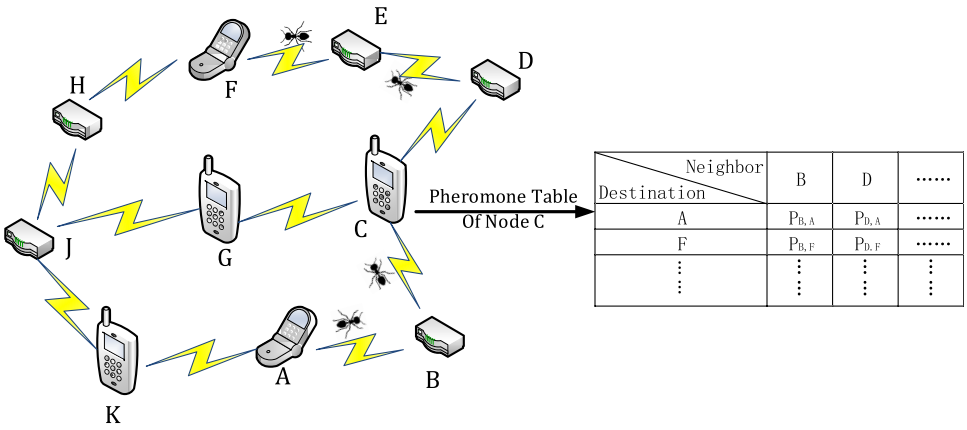


FIGURE 5. Example of Pheromone table.

of the current node, marked with L1, using SA. Each of the selected neighboring node shortlists 5 of its own neighboring nodes, marked with L2, also using SA. The best node of L2 is identified based on the trust values. Once the best L2 node is selected, the corresponding upstream node from L1 is also identified. Then the FANT moves to this identified node in L1. After each movement of the FANT, the trust values of all the links are updated. For links which the FANT hasn't visited, the trust values evaporate at a constant rate. The same methodology is repeated until the FANT arrives at the destination node or the maximum path length is reached. The novelty of this proposal is mainly that FANTs identify the next hop node by comparing trust values of 25 selected nodes in a two hop distance. Moreover, in order to find routes with minimal node reuse and to distribute the load through the network, this hybrid ACO routing protocol has incorporated randomness into the system to determine the paths. With the help of randomness during path selection, the energy depletion of certain centralized nodes is reduced. This enhances network stability further. However, the definitions of trust value related metrics, for example the stability, and the selection of the appropriate weight values for each metric are not clearly described.

6) SUMMARY

The energy reserve parameter used to be just one of many of QoS requirements, but in recent years it has become a popular topic in MANETs by itself. Repeatedly using the shortest path will drain the battery of the nodes on it, reducing their lifetime compared to other nodes. This will also decrease the lifetime of the network as a whole. The reviewed protocols in this section, all use the remaining battery power as a critical pheromone reinforcement factor to achieve high energy efficiency and extend the lifetime of the network. Another notable point is that most of the protocols in this section achieve lower energy consuming at the expense of the route discovery delay and the path length.

D. LOCATION AWARE ACO ROUTING PROTOCOLS

With the utilization of the Global Position System (GPS) [53], the location information of nodes becomes a popular issue when applying the routing protocols in practical. In this section we introduced six respective location aware ACO routing protocols in short. For more details, please read our previous work [11].

1) POSANT

Kamali and Opatrny [54] proposed an early reactive POSition based ANT colony routing protocol (POSANT) for MANETs. It combines the location information with traditional ACO routing algorithm, which aims to reduce the route establishment time while keeping less number of control messages. POSANT assumes that each node knows about its position, the position of its neighbors and the destination node. Then it uses the concept of zone which divides a node's neighborhood into three zones based on the physical location. For route discovery, the source node sends one FANT to each area on demand.

2) ROBUSTNESS-ACO

Unlike POSANT, Kadono *et al.* [55] have proposed a position aware ACO routing approach in MANETs which requires no location service. We abbreviate the proposed protocol as Robustness-ACO from here on. This paper constructs paths based on the robustness using the GPS information of visited nodes. The authors present two robustness functions to calculate the robustness value of a link. Based on this robustness value, the artificial ants decide the amount of pheromone to lay down. Each node predicts link disconnections by using the GPS information of its neighbors and redistributes the pheromone to accelerate alternative path construction. This mechanism is better adapted to dynamic network change and frequent link disconnection.

The successful implementations of ACO routing protocol in MANETs also inspire the application in Vehicle Ad hoc NETworks (VANETs). VANETs are the special

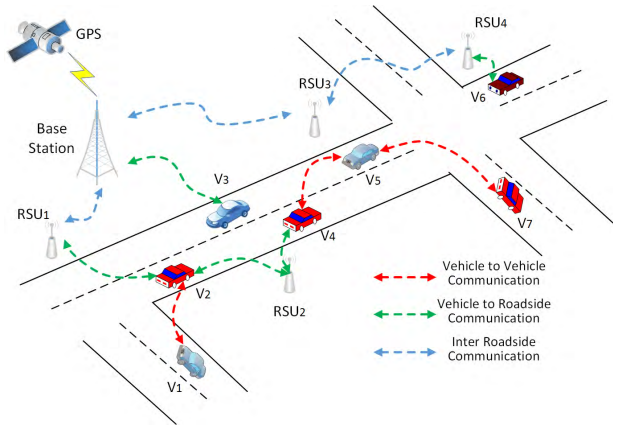


FIGURE 6. Communication in VANETs.

types of MANETs which gernerally consists of a network of vehicles, which are moving with a relatively high speed. Fig. 6 illustrates a typical communication pattern in VANETs. The devices located on the roads are called RSUs (Road Side Units) and the devices installed in the vehicles are called OBUs (On-Board Units). There are three communication types in VANETs [56]. The communication among vehicles, like V_4 - V_5 - V_7 and V_1 - V_2, is so called Vehicle-to-Vehicle (V2V) communication. The communication between vehicle and RSUs is Vehicle-to-Infrastructure (V2I) communication, like V_2 - RSU_1 and V_2 - RSU_2 - V_4. The communication among Road Side Units and Base Station is Inter Roadside Communication. In order to provide road safety, navigation, and other services, V2V and V2I co-exist in VANETs as shown in the Fig. 6.

3) MAR-DYMO

Correia *et al.* [56] have likely proposed the first ant-based algorithm that adapted to Dynamic MANETs On-demand (DYMO) routing protocol in vehicle ad hoc networks. The vehicles' information, such as speed and position, is applied to help updating the pheromone and making routing decision. Moreover, during the pheromone deposit process, MAR-DYMO uses Nakagami Fading Model [57] to indicate the path quality while utilizing Kinetic Graph framework [58] to show the link's stability. To our knowledge, this paper first implements ACO-DYMO in VANETs. However, this mechanism consumes large amount of bandwidth and is not scalable [59].

4) MAZACORNET

In [59] Rana *et al.* introduce a hybrid ant based routing protocol for VANETs that first divides the networks into zones to achieve scalability. To reduce broadcasting and congestion, they use a proactive approach within the zones to find routes and a reactive approach between zones. In MAZACORNET, the pheromone deposition and evaporation model is the same as with MAR-DYMO [56]. The difference is MAZACORNET uses five types of ants to discover the route within or outside the zone, and two routing tables to maintain the routing information. However, this paper does not explain how zones could be formed in a fast dynamic VANET. i

5) CLUSTER-BASED ACO

Unlike the flat architecture of the zone-based hybrid ACO routing protocol, a hierarchical approach for VANETs is proposed by Balaji *et al.* [60]. It combines a clustering architecture with ACO routing procedures to enhance the scalability with a better organization for the network. We abbreviate this protocol as Cluster-based ACO from here on. To achieve an efficient management, this protocol firstly divides the network into multiple virtual clusters by broadcasting a Member Packet (MEP). After autonomous clustering, ACO-DYMO routing procedures are employed in the same way as in MAR-DYMO [56]. One notable idea in this protocol is that it uses a reactive approach instead of using a hybrid approach which is otherwise commonly applied in cluster-based networks.

6) S-AMCQ

In recent year, Eiza *et al.* [61] have proposed a novel Secure Ant based Multi-Constrained QoS routing algorithm (S-AMCQ) for vehicle ad hoc networks, which considers not only QoS constraints, but also the security issues. In route discovery process, S-AMCQ applies ACO algorithm to explore numerous routes which satisfy multiple QoS constraints. And it uses an authentication mechanism to defend against external attackers. For the detection of internal attackers, S-AMCQ utilizes an extended VANET-oriented evolving graph (VoEG) model to perform plausibility checks on routing control messages. It also protects vehicles' privacy by using pseudonymous certificates. However, the authentication process in S-AMCQ is centralized and requires a Certification Authority(CA) that shows it is designed for V2I communications.

7) SUMMARY

The protocols introduced in this section represent a steady development of location aware ACO routing algorithms that leverage GPS. POSTAN [54] minimizes message delivery delay, while Robustness-ACO [55] combines robustness-based path construction with predictions of link disconnection. After the successful implementation in MANETs, many new ACO based routing protocols are also designed for VANETs. MAR-DYMO [56] guarantees both link quality and stability. In order to improve the performance, researchers focus on modifying MAR-DYMO into two architectures, namely zone-based and cluster-based architectures. MAZACORNET [59] subdivides the networks into zones to achieve scalability. A proactive approach is used within the zones while a reactive approach is applied between zones. Different from MAZACORNET, Cluster-based ACO [60] aims to reduce the number of routing control packets. However, message delivery in the network after the autonomous clustering is not described. S-AMCQ [61] considers both the

QoS constraints and the security issues to ensure reliable and robust routing in VANETs. In general, location aware ACO routing protocol have been well developed and show good prospects.

E. SECURITY AWARE ACO ROUTING PROTOCOLS

Other than QoS and energy efficiency, security is another hot topic in routing protocols which attracts many researchers' attention. As is well-known there exist many security threats in the network layer, such as black hole attacks, wormhole attacks, flooding attacks and so on. When these attacks are launched during the routing process, this usually leads to strong harmful effects on the network. In the worst cases, an attacker might even make the communication in the network impossible. Therefore, mechanisms that help participants in a network to defend against the potential attacks are necessary. However, the scope of security is wide. Different researchers have their own ideas about how to best build defense systems. In this section, an overview about existing security aware ACO based routing protocols is presented.

1) SAR-ECC

Vijayalakshmi and Palanivelu [62] have proposed a secure ant based routing algorithm for cluster based ad hoc networks using Elliptic Curve Cryptography (ECC [63]), which we abbreviate as SAR-ECC from here on. This approach makes use of two basic processes: one is estimating the trust value between neighbor nodes. The other uses the AntNet routing mechanism for route discovery and ECC for mutual authentication between the source and destination. In the network, each node in the cluster keeps trust values for all its neighbors. A trust value is calculated based on a measurement of uncertainty and is an increasing function that correlates with the probability of successfully transmitting each packet. During route establishment, the source node tries to find multiple routes using AntNet [30]. Then it gathers the trust values of all nodes in the paths. Based on the trustworthiness of nodes, it selects a trustworthy route for data transmission. The novelty of the protocol is using a trust value based on a measurement of uncertainty instead of the conventional pheromone. However, the updating mechanism for the trust value is not described and the benefits of combining a cluster structure with an ACO algorithm is not clearly described.

2) SPA-ARA

A secure power-aware reactive routing algorithm (SPA-ARA) inspired by ACO algorithms is proposed by Mehfuz and Doja [64]. SPA-ARA aims to not only manage energy usage, but also to guarantee security in MANETs. Similar to other ACO based routing protocols, SPA-ARA also launches ants to explore the network. Once a source node needs to send data packets to one destination node, it checks its pheromone table first. If there exists route information, it chooses the corresponding node as the next hop for which the next-hop availability is maximum. Afterwards, data packets secured by a Message Authentication Code (MAC) are transmitted along stochastically chosen routes by using the pheromone tables along the whole route. If there is no route information about the particular destination, the source node sends out reactive FANTs. These reactive FANTs are also attached with the MAC, which is generated using the HMAC keyed hash algorithm [65] with a shared group key. After receiving the reactive FANTs, intermediate nodes check first whether the attached MAC is valid. If it is correct, the intermediate node determines the trust value of the previous hop by looking it up in own trust pheromone table. Only if this trust value is above a predefined threshold value, the intermediate node accepts the FANT and establishes a secret key with the previous hop node by using a two-party key establishment protocol. This secret key is used for verifying the BANT later. As a consequence, a secret key is set up between each pair of neighboring nodes along the route. Once the destination node receives the FANT, it reacts analogously to the intermediate nodes. Only if the FANT has a valid MAC and the trust value of the previous hop is above the threshold, the destination node generates a corresponding BANT. Otherwise, it discards the FANT without taking any further action. This BANT is secured with a MAC generated with the secret key between the destination node and the next hop in the path towards the source node. Intermediate nodes verify the MAC attached to the BANT by using the corresponding secret keys hop by hop. When the BANT successfully arrives the source node, it has also updated all the pheromone tables along its journey. Based on the attached MACs and pairwise secret keys, the ants finish the authentication process in the reactive path setup phase. The authors have written that SPA-ARA could protect the network from most common attacks on routing protocols for ad hoc networks and have compared its performance with the Source Routing Protocol (SRP) [66] protocol. The results show that SPA-ARA has longer lifetime than SRP, and attackers lead to less dropped packets in SPA-ARA. In order to maximize network lifetime, the number of hops, travel time and the batteries' remaining energy are chosen as the optimization parameters, which directly affect the pheromone updating process. Going from these results, SPA-ARA has the lowest energy level standard deviation when compared to the AODV [2], DSR [3] and ARA [31] protocols. It also discovers the most successful routes. The proposed scheme pays attention not only to security, but also to the nodes' remaining energy so as to achieve a fair distribution of energy usage. Due to the cryptographic mechanism frequently used in the MAC and when broadcasting FANTs in the route discovery phase, overhead is one of most critical parameters for evaluating the performance of the proposed routing protocol. However, the authors haven't shown any results regarding overhead.

3) FTAR

Fuzzy logic has been widely utilized in many areas of our daily life. Since the 1980s, many fuzzy logic based systems

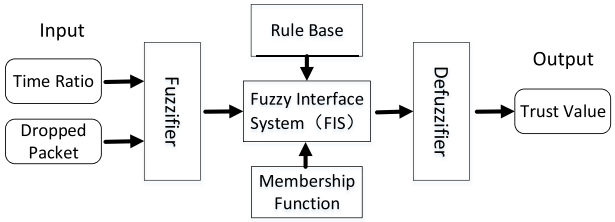


FIGURE 7. Block Diagram of fuzzy system for estimating trust.

have been proposed in many fields, such as automatic control, automobile production, academic education, industrial manufacturing and so on. Due to its great success, researchers [67], [68], [69], [70] have designed new routing protocols in MANETs, combining fuzzy logic with ACO algorithms. Sethi and Udgata [71] have proposed a fuzzy-based trusted ant routing (FTAR) protocol in 2011. FTAR combines swarm intelligence and the fuzzy system to select the optimal path. In the route discovery phase, FTAR follows the same concepts as those used in many other conventional ACO routing protocols. FANTs travel through the network hop by hop using Blocking Expanding Ring Search (Blocking-ERS) [41]. In order to prevent cycles in the path, each intermediate node stores recently forwarded route requests in a buffer. BANTs follow back tract along the routes of their corresponding FANTs until they reach the source node. After pheromone tracks are established between source and destination nodes, data packets update the pheromone values along the path while they are transmitted to the destination node. If there is no data communication in the network, pheromone values evaporate with the time. If a node doesn't receive an acknowledgment within predefined interval, it generates a route error message and the pheromone value of the related routes reduce to 0. In other words, the routes are deactivated. Meanwhile, the node tries to deliver the data packet to the destination via alternative routes. If the data packet couldn't reach the destination, then the source node has to search for new routes. FTAR aims to distinguish between healthy and malicious nodes, and has introduced a fuzzy-based trusted node model. In this model each node is assigned a trust value signifying its trustfulness. As shown in Fig. 7, input parameters for the fuzzy control are chosen to be the dropped packets and time ratio, which represents the ratio between the route reply time and the time -to-live. The membership functions of the two input and single output parameters are assumed to be Gaussian functions. Each input parameter is categorized into four levels; and the output parameter is appraised by five levels. A series of IF-THEN rules are defined for the fuzzy inference system. The Smallest Of Minimum (SOM) is applied for the defuzzification process. After the fuzzy process, the fuzzy trust value is evaluated. It can affect the route discover phase, because FANTs only choose trusted neighbor nodes on their paths. In the presence of unsafe or malicious nodes, the results show an improvement over the Ant-U algorithm. However, the authors have not given a detailed explanation of the relationship between their fuzzy based trust value and the pheromone value in the ACO structure. The approach is apparently structured as two separate systems working together.

4) SBDT

Indirani and Selvakumar [72] have proposed a Swarm Based intrusion detection and Detection Technique (SBDT) in 2012. It uses the swarm intelligence of ant colony optimization to establish multiple paths between source and destination nodes. Nodes with high trust values, residual bandwidth and energy are selected as active nodes (NAs). Each NA monitors its neighbor nodes and collects all their trust values. NAs also exchange the gathered trust values with their neighbor NAs. If a node's trust value is below a predefined minimum trust value, the NAs marke it as malicious. Upon detecting a malicious node, the NA node informs a transmission's source node about the detection. In order to defend against the malicious node, the source node performs a key revocation process. In this approach, the trust value is a core factor to support the whole detection system. However, the authors haven't mentioned how the trust values are estimated and updated.

5) DBA-ACO

Other than designing intrusion detection systems, researchers are also interested in preventing certain attacks. Sowmya *et al.* [73] have proposed an idea to prevent black hole attacks using the ACO routing structure, which we abbreviate as DBA-ACO from here on. The approach follows the conventional ACO routing protocols to discover routes. In order to detect black hole node, a dynamically updated threshold value is used. The threshold value is the average difference of the destination sequence numbers in the routing table and those brought back by the BANTs. If a BANT brings back a destination sequence number which is higher than the threshold value, the node who forwards this BANT is then considered a black hole node. Once a black hole node is detected, alarm packets with the black hole node's ID are distributed through the network. Hence, the nodes of the network can isolate the malicious node. This approach avoids the usage of any cryptographic mechanisms to ensure security in the routing protocol. However, the authors have not performed any simulation to test the performance of the proposed idea.

6) ANTNET

Pal *et al.* [74] have found another way of detecting black hole attacks. They apply ACO to the AODV [2] routing mechanism, calling it ANTNET. This protocol first uses AODV to gather paths and then applies the ANTNET algorithm to detect the anomalies. Finally, it uses the ACO mechanism to rediscover paths. However, the update mechanism of the pheromone is not mentioned and there is no description about the concrete reactions after detecting the black hole nodes.

7) ABPKM

Memarmoshrefi *et al.* [75] have proposed an Autonomous Bio-inspired Public Key Management (ABPKM) approached for MANETs to defend against network layer attacks. The main idea is to apply ACO for self-organized public key management to prevent nodes' misbehavior and ensure the correctness of the public keys. The trust value in this approach is estimated based on identity assurance, which means the level at which the public key being presented can be trusted to represent a particular node and not some other nodes in the network. In order to combine the trust based public key mechanism with an ACO algorithm, the authors use the trust value as the pheromone value in the ACO algorithm. The proposed approach consists of four main parts: the initialization phase and certificate issuing, the certificate chain discovery, the public key authentication by certificate verification and the certificate chain trust/pheromone update. In first phase each node issues public key certificates to its neighboring nodes upon receiving their public keys and the initial trust/pheromone value to all issued certificates are set with the threshold value 0.5. Once a source node wants to authenticate the public key of a destination node, the source node sends out FANTs to find desired certificate chains from the source node to the destination node. The route discovery process is similar to that of conventional ACO routing protocols, except the BANTs also carry certificate chains. After the source node has found the certificate chains, it needs to authenticate the public key represented by those chains. It retrieves the public key of the destination node from the received chains and computes the corresponding trust values of the chains. The route represented by the chain with highest trust value is chosen for data transmission. Based on the results of the public key authentication process, the source node updates the trust values of its neighboring nodes. The updating is launched hop by hop along the chains. Nodes in a chain without any fake certificate are rewarded with increasing trust values. In contrast, nodes in a chain which includes fake certificates are punished by their upstream nodes. In this paper, the authors have investigated the scalability and robustness of ABPKM by varying network size, mobility and the percentage of malicious nodes. The simulation results show that ABPKM provides good performance over a wide range of scenarios and remains stable for all tested network sizes. The novelty in this protocol is connecting the trust value from public key management with the pheromone in ACO algorithms. This design lets ABPKM reap benefits from both sides. After their first design, the authors have improved the model in [76] to detect more complex attacks, such as Sybil attacks, during the public key authentication phase. They add the agglomerative hierarchical clustering algorithm to ABPKM and analyze the nodes' behavior with a new Sybil attack detection model. Based on the gathered certificate chains, the source node extracts node features, such as the number of groups one node belongs to, the distance of a node to the destination node, the social degree of one node and the average trust value for the chains in which the node participates. These features help the source node to group other nodes during the clustering process. Another interesting parameter - inspired from mate and non-mate discrimination in real ant colonies - the aggression value, is also newly introduced in the model. This value is used to estimate the danger level of one node in the network. After the clustering process, the node's aggression values are estimated. In their following work [77], they give additional simulation results. These show, based on an experimentally determined best cutoff point and aggression threshold values respectively for different network sizes, that moving nodes have a generally better accuracy for detecting the attacker nodes. However, these results are from the learning phase of the ACO based autonomous authentication model. The performance of a complete routing protocol including the proposed detection mechanisms still needs to be investigated.

8) SUMMARY

In this section we have surveyed some of the existing security aware ACO based routing protocols in chronological order. Based on the aims of these protocols, they can be divided into two groups: general and targeted, as shown in Fig. 4. The first group aims to generally detect anomalies in the network, while the other one targets a particular attack (e.g. black hole attacks). If we only focus on the security model applied in these protocols, 71% of them are trust based models. There are different ways to set up trust models. Sethi and Udgata [71] have applied the fuzzy logic to estimate the trust values in their protocol FTAR, while the other researchers [62], [64], [75] have applied authentication mechanisms to create their own trust models. From our observations, we infer that the combination of fuzzy logic and ACO could be well suited to improving the security in MANETs. However, choosing suitable parameters which should be considered in the fuzzy system is very important in order to estimate accurate trust values. The choice may be strongly influenced by the design aims of the protocol and also related to the experiences obtained by the designer. For example, the rule base which is used within a fuzzy system is usually made by experience and it can strongly affect the output results. We are looking forward to more research which explores or discusses these open issues in this area. Authentication mechanisms are an important feature used to improve the security in wireless networks. 80% of the trust based models in this section have applied such mechanism. SPA-ARA [64] is one representative example of an authentication based approach in this section. The authors have pointed out that SPA-ARA can detect most of the common attacks in MANETs. However, due to the cryptographic mechanism frequently used for authentication, overhead is one of the most critical parameters for evaluating the performance of the proposed routing protocols.

F. OTHER ACO BASED ROUTING PROTOCOLS

Instead of focusing only on a single issue such as QoS, energy, security, etc., researchers have also proposed other ACO based routing protocols which consider two or more

TABLE 1. Design parameter overview of basic ACO routing protocols.

Protocol	Routing Approach	Tran. Type FANT	Ph. Activator
AntNet [30]	proactive	unicast	BANTs
ARA [31]	reactive	broadcast	FANTs, BANTs, DPs
PERA [32]	proactive	unicast	BANTs
AntHocNet [33]	hybrid	both	RBANTs, PBANTs
PACONET [35]	hybrid	broadcast	FANTs, BANTs
ACO-AHR [36]	hybrid	both	service agents
HOPENT [37]	hybrid	unicast	FANTs, BANTs
Ant-E [40]	reactive	broadcast	FANTs, BANTs, DPs

TABLE 2. Pheromone parameter overview of basic ACO routing protocols.

Protocol	Design Goals	Ant Types	Pheromone	
			Reinforcement	Evaporation
AntNet [30]	distributed, robust, multi-path routing	FANT, BANT	goodness of trip time	goodness of trip time
ARA [31]	reduce overhead	FANT, BANT	hop count	constant rate
PERA [32]	reduce overhead	FANT, BANT, uniform FANT	delay, hop count, trip time	delay, hop count, trip time
AntHocNet [33]	efficient routing	PFANT, PBANT, RFANT, RBANT, RPFANT, RPBANT	hop count, delay	constant rate
PACONET [35]	efficient dynamic routing	FANT, BANT	travel time, run time parameter	constant rate
ACO-AHR [36]	apply multi-agents to reduce expense	FANT, BANT	travel time, ant release ration	constant rate
HOPENT [37]	high scalability, less overhead	IFANT,EFANT, BANT,NANT,EANT	travel time	constant rate
Ant-E [40]	control overhead, improve reliability	FANT, BANT	hop count	constant rate

issues in the same time. In previous sections we have already reviewed some of them. For instance, SPA-ARA [64], introduced in Section III-C, considers both energy and security in the routing process. Another example is S-AMCQ [61] in Section III-D, which considers the QoS and security in VANETs communication. Considering multiple issues in a routing protocol's design can make the protocol more suitable for real world applications. However, this is a new direction that has not been investigated by many researchers yet. Therefore, we just point them out in this section instead of categorizing them into a separate group. However, we infer that designing ACO routing protocols based on the multiple existing issues in MANETs and especially in VANETs, would be an interesting future research direction.

IV. ANALYTICAL COMPARISON OF ACO BASED ROUTING PROTOCOLS FOR MANETs

In the previous section, we have reviewed some of the existing ACO based routing protocols and identified five main directions. In this section we summarize and compare the previously surveyed ACO based routing protocols, covering the time from 1998 to 2016. We focus on comparing the design patterns of these ACO-based routing protocols. Ten tables in this section show an analytical comparison of all the protocols according to the categories introduced in the previous section: basic optimization, QoS awareness, location awareness, energy awareness and security awareness.

A. ANALYTICAL PARAMETERS

We have chosen the following seven parameters to compare the different ACO based routing protocols:

Design Goals: This parameter explains the aims of the proposed protocols. The goals usually indicate the categories which the routing protocol belongs to.

Ant Types: In conventional ACO based routing protocols, there are usually two types of ants: FANTs and BANTs. However, depending on the design of the protocols, there could be other types of ants in the network. This parameter lists all types of ants in the protocol.

Pheromone Reinforcement Factors (Ph. Reinforcement): Pheromone is one of the most important parts in ACO based routing protocols. This parameter specifies what is considered while reinforcing the pheromone values in the algorithm.

Pheromone Evaporation Factors (Ph. Evaporation): In ant colonies pheromone evaporates over time. This allows ants to forget old paths. This parameter specifies what is considered while evaporating the pheromone values in the algorithm.

Routing Approach: This parameter signifies if the routing protocol is proactive, reactive or hybrid.

Transmission Type of FANTs (Tran. Type FANTs): This parameter explains the type of transmission for FANTs. The types used in all reviewed protocols in this work are unicast and broadcast.

Pheromone Update Activators (Ph. Activators): Pheromone in ACO based routing protocols changes dynamically. This parameter explains where the pheromone is updated in the routing protocol.

We divide the parameters mentioned before into two groups, for example, as shown in Table 1 and Table 2: the common basic design properties and the pheromone related core design properties. The first group introduces the basic routing structure, while the other group reflects the core ACO mechanism within the routing protocol.

In the following subsections, we present our observations in the form of these two kinds of comparison tables, dividing up the algorithms according to five categories that we've previously introduced. In addition, each section's results are summarized.

B. COMPARISON OF BASIC ACO ROUTING PROTOCOLS

In Table 1, we have summarized various basic optimization ACO-based routing protocols for MANETs. Many of them are representative algorithms in this category, such as AntNet [30], ARA [31], etc. Routing protocols could be classified into proactive, reactive and hybrid approaches, which is listed in the path establishment column. Overall, 75 % of the studied protocols in this category have a reactive or hybrid routing design, instead of using a proactive design, which usually causes more overhead for maintaining routing tables. This trend reflects the requirements of ad hoc network. Generally speaking, broadcasting a message produces more control messages, because the message needs to be transferred to all recipients simultaneously. On the contrary, using unicast method the message is sent to exactly one destination device. However, it has a relatively lower probability of finding global optima. 37.5 % of the reviewed protocols broadcast FANTs and another 37.5 % prefer unicasting them. It is also noteworthy that the remaining protocols, namely AntHocNet [33] and ACO-AHR [36], switch between unicast and broadcast type, based on whether there is any routing information about destination nodes. A less common way of updating pheromone values is presented in ARA [31] and Ant-E [40] where data packets update the pheromone and in ACO-AHR [36], where service agents take over this duty.

After having an overview of the common design properties, we look more closely to the properties of the pheromone applied in these ACO based routing protocols. Table 2 includes some representative ACO algorithm related parameters: design goals, ant types, the pheromone reinforcement factor(s) and the pheromone evaporation factor(s). From Table 2, the listed early basic optimization routing protocols aim to efficiently find optimal routes with limited routing overhead. Most of the studied protocols use two kinds of ants, FANTs and BANTs. Due to different requirements in the reactive and proactive routing phases, many hybrid protocols use more than two types of ants. For example, in HOPNET [37], there are four other types of ants: Internal FANTs (IFANTs), External FANTs (EFANTs), Notification ANTs (NANTs) and Error ANTs (EANTs). The way in which pheromone values are calculated differs among the listed protocols. The metrics used for reinforcing the pheromone are usually hop count, ant's travel time, end to end delay and path goodness. Most of the protocols consider a combination of these metrics with separate weights, according to the requirements imposed by the protocol design. The pheromone evaporation process is based on evaporation factors which can be dynamic or static. Examples of the dynamic evaporation factors are the goodness of trip time factor used in AntNet [30]. The most common evaporation factor is a predefined constant rate.

C. COMPARISON OF QoS AWARE ACO ROUTING PROTOCOLS

Quality of Service is the primary mission for data transmission and communication in MANETs. In Table 3, we focus on basic properties of the selected four QoS aware ACO based routing protocols. Similar to the result from Table 1, 75 % of the studied protocols in this section have designed the protocol with a reactive or hybrid structure. ARAMA [42] as an early protocol is a proactive approach and SAMP-DSR [43] is a hybrid protocol. The recent protocols prefer to use reactive approaches such as QAMR [44] and QoRA [45], because they adapt better to real-time communications. The rest of table shows that half of the protocols broadcast FANTs while the other half unicast them. Only QAMR uses both FANTs and BANTs to update the pheromone while the others use just BANTs or RREQs, which are Route REQuest packets.

As shown in Table 4, all the surveyed protocols aim mainly to ensure link stability and optimize hop count. QoRA attempts to reduce overhead produced by control messages or without synchronization. Parameters related to QoS such as delay, remaining battery energy, end to end reliability and bandwidth are considered as pheromone reinforcement factors in these protocols. Most of the reviewed protocols in this subsection use a constant rate to evaporate the pheromone except ARAMA which estimates the path grade and uses it as an evaporation factor.

D. COMPARISON OF ENERGY AWARE ACO ROUTING PROTOCOLS

The limited battery power of nodes in ad hoc networks is one critical issue. Repeatedly using the shortest path will drain the battery of the nodes on it and decrease the lifetime of the network as a whole. For this reason energy efficiency has become a hot issue in designing routing protocols rather than being just one of many QoS requirements. In this subsection, we focus on efficient, energy aware routing protocols. Table 5 and 6 present the details of our comparison in this area.

Table 5 shows that only 40 % of the protocols set up routes proactively. While BANTs are usually unicast from

TABLE 3. Design parameter overview of QOS aware ACO routing protocols.

Protocol	Routing Approach	Tran. Type FANT	Ph. Activator
ARAMA [42]	proactive	unicast	BANTs
SAMP-DSR [43]	hybrid	unicast	RREQs
QAMR [44]	reactive	broadcast	BANTs, FANTs
QoRA [45]	reactive	broadcast	BANTs

TABLE 4. Pheromone parameter overview of QOS aware ACO routing protocols.

Protocol	Design Goals	Ant Types	Pheromone	
			Reinforcement	Evaporation
ARAMA [42]	Optimize hop counts and QoS, energy efficient	FANT, BANT	queue delay, remaining battery energy, link's signal to noise ratio, bit error, path grade	path grade
SAMP-DSR [43]	Solve the shortcoming of ACO and DSR	FANT, RREQ	end to end reliability, the trip time	unknown
QAMR [44]	Achieve link stability	FANT, BANT	bandwidth, delay, hop count	constant
QoRA [45]	less further control messages or without synchronization	FANT, BANT, EANT	constant	constant

TABLE 5. Design parameter overview of energy aware ACO routing protocols.

Protocol	Routing Approach	Tran. Type FANT	Ph. Activator
ACO-EEAODR [48]	reactive	broadcast	REPs
EAAR [49]	reactive	broadcast	BANTs
AntHocMMP [50]	proactive	unicast	FANTs, BANTs
ACECR [51]	proactive	broadcast	BANTs
Hybrid ACO [52]	reactive	unicast	FANTs

TABLE 6. Pheromone parameter overview of energy aware ACO routing protocols.

Protocol	Design Goals	Ant Types	Pheromone	
			Reinforcement	Evaporation
ACO-EEAODR [48]	increase network lifetime	RREQ, RREP	remaining battery power	unknown
EAAR [49]	less energy consumption, multi-path transmission	FANT, BANT	MBR, hop count	constant rate
AntHocMMP [50]	path robustness, extend network lifetime	FANT, BANT	energy path cost	constant rate
ACECR [51]	extend network lifetime	FANT, BANT	avg. & min. energy, hop count	constant rate
Hybrid ACO [52]	secure, energy efficiency	FANT	predefined constant	constant rate

the destination back to the source, FANTs are either broadcast or unicasted hop by hop. 60 % of the reviewed protocols in this subsection update pheromone after ants have reached their destinations. The concrete pheromone update activators in these protocols are either BANTs or RREPs. Besides BANTs, AntHocMMP [50] also uses FANTs to update pheromone values. Hybrid ACO doesn't specify the type of ants it uses. Pheromone updates occur before ants have reached the destination nodes. Therefore, it's similar to the protocols which use FANTs as the pheromone update activators. Table 6 shows that the main purpose of all energy efficient protocols is to extend the whole network's lifetime by reducing repetitive use of the same nodes in shortest paths. For pheromone reinforcement, Hybrid ACO just uses a predefined constant amount, while ACO-EEAODR [48] considers only the remaining battery power for updating pheromone values. ACECR [51] considers both the average energy and minimum energy of a path to select a path with more residual energy on a global view. Both EAAR [49] and AntHocMMP consider the Maximum of minimum Residual Battery power (MRB) of all nodes in a path. The difference between them is that EAAR uses MBR as a pheromone reinforce factor while AntHocMMP uses it to find relative paths.

E. COMPARISON OF LOCATION BASED ACO ROUTING PROTOCOLS

In this subsection, we describe the different parameters for the location aware ACO routing protocols in Table 7 and 8.

TABLE 7. Design parameter overview of location aware ACO routing protocols.

Protocol	Routing Approach	Tran. Type FANT	Ph. Activator
POSANT [54]	reactive	unicast	BANTs
Robustness-ACO [55]	hybrid	broadcast	FANTs,BANTs
MAR-DYMO [56]	reactive	broadcast	RREPs
MAZACORNET [59]	hybrid	unicast	unknown
Cluster-based ACO [60]	reactive	broadcast	RREPs
S-AMCQ [61]	reactive	unicast or broadcast	RQANTs

TABLE 8. Pheromone parameter overview of location aware ACO routing protocols.

Protocol	Design Goals	Ant Types	Pheromone	
			Reinforcement	Evaporation
POSANT [54]	Min. delivery delay	FANT,BANT	distance,location	constant rate
Robustness-ACO [55]	construct robust paths	Hybrid FANT/ BANT	robustness,cost	constant rate
MAR-DYMO [56]	adapt ACO to VANETs	Hello message, RREQ/RREP	reception probability, lifetime ratio	path lifetime
MAZA-CORNET [59]	scalability,robust to link failures	IFANT,EFANT, BANT,NANT, EANT	same with MAR-DYMO	same with MAR-DYMO
Cluster-based ACO [60]	improve MAC layer efficiency	Hello message, RREQ/RREP	same with MAR-DYMO	same with MAR-DYMO
S-AMCQ [61]	ensure reliable, robust routing	RQANT,RPANT REANT	QoS metrics, reliability value	individual variable

Table 7 shows that all the reviewed protocols avoid to apply the proactive approach, due to the overhead caused by proactively maintaining of routing tables. As for the transmission type of FANTs, ca. 50 % of all approaches broadcast FANTs while the remaining protocols except S-AMCQ, unicast FANTs. S-AMCQ broadcasts the routing control ants only when there is insufficient information available at the pheromone table. In the pheromone update phase, only in the Robustness-ACO protocol both FANTs and BANTs can update the pheromone. Utilizing the location information from GPS helps ACO based routing protocols adapt better to MANETs, especially to VANETs. The main goals of many reviewed protocols in this subsection are to minimize delivery delay and establish robust routes. Various ant types are used in these approaches. Other than the basic FANTs and BANTs, there are internal FANTs (IFANTs), external FANTs (EFANTs), Notification ANTs (NANTs) and Error ANTs (EANTs) in protocols which are designed for hierarchical networks, such as MAZACORNET. In some of the reviewed protocols, RREQs and RREPs are also used in the route discovery phase. Hop count and the cost of a route are two main pheromone reinforce factors in MANETs. In VANETs, however, this can be quite different due to frequent interruptions of paths. References [56], [59], and [60] in the VANETs scope use the probability of reception of a message, the ratio between the estimated lifetime of a path and the maximum allowed lifetime of a path, to update the pheromone. The protocols in MANETs use a constant rate for pheromone evaporation, while the VANETs protocols use the lifetime of a path or an individual variable value [61] to reduce the pheromone values.

F. COMPARISON OF SECURITY AWARE ACO ROUTING PROTOCOLS

Due to the prevalence of security threats in the networks, security is also a hot topic that attracts many researchers' attention. Common attack types are, for example, black hole and wormhole attacks. Different researchers have proposed various ideas about how to ensure security in their routing protocols. In this section, we compare a selection of security aware ACO based routing protocols. These protocols use several methods to ensure secure routing. From Table 9, we observe that all surveyed protocols in this subsection use reactive approaches, thus avoiding the higher overhead commonly associated with proactive methods. For example, besides the regular proactive routing table maintenance, if a malicious node is detected in proactive approaches, all nodes in the network need to put the malicious node into black lists and update their routing tables to avoid routes including the reported malicious node.

Table 10 shows that most of the security aware ACO routing protocols aim to ensure finding secure and reliable routes. Some of them such as DBA-ACO [73] and ANTNET [74] focus on defending against certain attack types, while others are interested in detecting malicious or anomalous nodes in the network. All the listed protocols use the basic ant types, except ABPKM [75] which has two other special ant types, namely Repair ANTs (RANTs) and Update ANTs (UANTs). Although some of the proposed protocols have not described their pheromone related parameters clearly, we can still observe that there are various pheromone reinforcement factors, which are applied in this subsection. Besides a trust value, which is the most common parameter, there are also other parameters used for reinforcing the

TABLE 9. Design parameter overview of security aware ACO routing protocols.

Protocol	Routing Approach	Tran. Type FANT	Ph. Activator
SAR-ECC [62]	reactive	unicast	unknown
SPA-ARA [64]	reactive	both	BANTs
FTAR [71]	reactive	broadcast	FANTs
SBDT [72]	reactive	unknown	unknown
DBA-ACO [73]	reactive	unknown	unknown
ANTNET [74]	reactive	unknown	ANTs
ABPKM [75]	reactive	unicast	BANTs

TABLE 10. Pheromone parameter overview of security aware ACO routing protocols.

Protocol	Design Goals	Ant Types	Pheromone	
			Reinforcement	Evaporation
SAR-ECC [62]	secure routing	FANT, BANT	trust value	unknown
SPA-ARA [64]	energy efficiency, detect malicious nodes	FANT, BANT	distance, traveling time	constant rate
FTAR [71]	trusted routing	FANT, BANT	constant rate	constant rate
SBDT [72]	detect malicious nodes	FANT, BANT	unknown	unknown
DBA-ACO [73]	detect and prevent black hole attack	FANT, BANT	unknown	unknown
ANTNET [74]	detect and prevent black hole attack	ANT	trails, attractiveness	unknown
ABPKM [75]	secure self-organized authentication routing	FANT, BANT, RANT, UANT	trust value	constant rate

pheromone values, such as traveling time, distance, trails and attractiveness. In contrast to the reinforcement factors, most of the protocols use a constant rate to evaporate the pheromone over time.

V. SIMULATION PARAMETER COMPARISON OF ACO BASED ROUTING PROTOCOLS

A. COMPARISON OF IMPLEMENTATION RELATED METRICS

Table 11 shows the representative performance metrics of the surveyed protocols in the five main categories. As can be seen in Table 11, nearly 97% of the surveyed protocols have implemented their ideas and evaluated their performance of these, ca. 83% are implemented in common simulators, such as NS2 [78], GloMoSim [38]/ QualNet [34], OMNet++ [80] and so on. Around 10% protocols are implemented in self-developed simulators. Around 83% of the studied protocols have compared their performance to that of other standard routing protocols for MANETs. AODV [2] is one of the most popular protocols chosen for comparison in earlier publications. After being presented to the public, AntHocNet [33] also becomes a benchmark ACO routing protocol commonly used for comparison.

In order to evaluate the performance, researchers mainly focus on the Data Delivery Ratio (DDR), the end to end delay and the routing overhead. 80% of the studied protocols have shown results for at least one of these three metrics. Moreover, nearly 79% of the protocols in the basic and location aware ACO routing categories have evaluated all these three metrics. In the location aware ACO routing category this value even rises to 100%. Meanwhile, the percentage of protocols which don't consider any special performance metrics in these two categories are 50% and 40% respectively. In the other three categories these values are much lower. This indicates that basic and location aware ACO routing protocols consider these three metrics as important performance metrics.

In contrast, the other three categories have more special performance metrics due to their design aims. Besides the previously mentioned metrics, data throughput, the scalability of the network and the hop counts of connections are the most popular metrics used by many protocols from all the five main categories. Moreover, we have observed that there are some other particular special metrics for different categories due to their special pertinence. For example, in the energy aware ACO routing category, ACO-EEAODR [48] and EAAR [49] have not illustrated any common metrics. ACO-EEAODR only compared the energy consumed in path selection and the network lifetime. EAAR uses six performance metrics for the comparison of their protocols with others, which are the number of dead nodes, the number of packets dropped, the total energy consumed, the number of packets delivered, the energy per packet delivered, the packets delivered per dead node and the packets dropped per packets delivered. The network lifetime, the dead node ratio and the energy consumed are the most popular performance metrics for all surveyed protocols in this category.

In the security aware ACO routing category there are also many special metrics. Except for DBA-ACO [73], which has no implementation, all of the other protocols in this category are evaluated using special metrics. Moreover, 50% of these protocols have only focused on evaluation using their own special performance metrics. For instance, in SBDT [72], the authors have shown the detection accuracy which

TABLE 11. Simulation parameter overview of ACO based routing protocols.

	Protocol	Compare with	Simulator	DDR	Delay	Overhead	Special
Basic	AntNet [30]	OSPF,SPF,BF, Q-R,PQ-R, Daemon	own simulator [30]	NO	YES	YES	YES
	ARA [31]	AODV, DSDV,DSR	NS2 [78]	YES	NO	YES	NO
	PERA [32]	AODV	NS2	NO	YES	NO	YES
	AntHocNet [33]	AODV	QualNet [34]	YES	YES	YES	YES
	PACONET [35]	AODV	GloMoSim [38]	YES	YES	YES	NO
	ACO-AHR [36]	AODV	NS2	YES	YES	YES	NO
	HOPENT [37]	AODV,ZRP, AntHocNet	GloMoSim	YES	YES	YES	YES
	Ant-E [40]	AODV,ZRP, AntHocNet	NS2	YES	YES	YES	NO
QoS aware	ARAMA [42]	without	OPNET [79]	YES	NO	NO	YES
	SAMP-DSR [43]	EMP-DSR,MP-DSR, AODV,AntHocNet	OMNet++ [80]	YES	YES	YES	NO
	QAMR [44]	AODV, ARMAN	NS2	YES	NO	YES	YES
	QoRA [45]	AODV, CLWPR	NS-3 [81]	YES	YES	NO	YES
Energy aware	ACO-EEAODR [48]	EEAODR	GloMoSim	NO	NO	NO	YES
	EAAR [49]	AODV,MMBCR, AntHocNet	GloMoSim	NO	NO	NO	YES
	AntHocMMP [50]	AntHocNet,LAR, R-ACO1,MMP	NS2	YES	YES	YES	YES
	ACECR [51]	AOMDA, EAAR	NS2	YES	YES	NO	YES
	Hybrid ACO [52]	Normal ACO	unknown	NO	YES	NO	YES
Location aware	POSANT [54]	AntNet, GPSR, AntHocNet	own simulator [54]	YES	YES	YES	NO
	Robustness-ACO [55]	AntHocNet, LAR	own simulator [55]	YES	YES	YES	YES
	MAR-DYMO [56]	AODV,DYMO, Ant-DYMO	NS2, VNMG [82]	YES	YES	YES	NO
	MAZA-CORNET [59]	AODV,AMODV, GPSR	NS2, VanetMobiSim [83]	YES	YES	YES	YES
	Cluster-based ACO [60]	AODV	NS2,VNMG	YES	YES	YES	YES
	S-AMCQ [61]	IAQR [84],AMCQ [61]	OMNet++	YES	YES	NO	YES
Security aware	SAR-ECC [62]	without	NS2	NO	NO	NO	YES
	SPA-ARA [64]	AODV,DSR,ARA	SWANS [85]	NO	NO	NO	YES
	FTAR [71]	ANT-U	NS2	YES	YES	YES	YES
	SBDT [72]	CAPMAN	NS2	YES	YES	NO	YES
	DBA-ACO [73]	without	NO	NO	NO	NO	NO
	ANTNET [74]	without	NS2	NO	NO	NO	YES
	ABPKM [75]	without	QualNet	YES	YES	YES	YES

represents how well the algorithm detects security threats. In SAR-ECC [62] the authors have presented the successful rate of packet forwarding, the authentication cost and the necessary packet rate vs. the speed of nodes. Another protocol SPA-ARA [64] also shows the energy consumption, the number of successfully found routes and the number of packets dropped by the malicious nodes. From observations, we infer that security aware ACO routing protocols consider the security related metrics more important than the general benchmarking metrics, such as end to end delay. In other words, in order to guarantee security during network communication, these protocols made a trade-off between the security level and performance. However, due to the different scope aimed at by these protocols targeting various security issues, there are not many common special performance metrics. This could be a reason to answer the question why 50% of protocols in this category have not made any comparison with related work.

Another observation we have found is that although many of the surveyed protocols have shown good performance in small networks, the scalability of the proposed protocols has not been demonstrated. In contrast, in [71] the authors have shown the DDR, delay and overhead metrics over increasing the network sizes and mobility rates respectively. Besides the common performance metrics related to the scalability, in [75] the authors have also shown the successful rate of finding certificate chain, the reliability of selected honest certificate chains and other special metrics which describe the performance of the proposed approach.

From the reviewed ACO based routing protocols in this paper, it can be clearly seen that significant efforts have been made to address the requirements of efficient and effective routing protocols for MANETs. The results of our comparison based on protocol design and simulation parameters are presented in Section IV and V. We have also identified certain drawbacks in the considered routing protocols. First of all, most of the reviewed approaches in all five categories have not been evaluated with large networks. Although all the surveyed protocols have shown good performance in small networks, the scalability of the proposed protocols has not been demonstrated. Secondly, most of the location aware protocols have not mentioned security or authentication and all the proposed protocols in VANETs completely lack practical testing via real-time traffic models. Finally, in the security based ACO routing category, more than 50% of the protocols only do self analysis and no comparison with other standard routing protocols are done.

B. DISCUSSION

In this section we summarize the development history of the five main categories and discuss future possible design directions of ACO based routing protocols.

Fig. 8 shows the development history of all surveyed papers of the five main categories in the past 19 years. Designing effective and efficient protocols to address only the basic requirements of routing in MANETs used to be a hot topic. Due to the dynamic nature of ACO's connectivity, ACO is able to continuously find the optimal routes in real time despite the topology changes in the network. Therefore, researchers began to apply ACO algorithm to solve the routing problem in MANETs. The first ACO based routing protocol was proposed in 1998. Since then many subsequent researchers have focused on this direction for more than ten years. In the early blossoming stage of ACO based routing algorithms, QoS in routing was an important aspect in MANETs and until now QoS based ACO routing protocols have been studied for over than 13 years. The other three categories shown in Fig. 8 are relatively new directions which have been developed within the last ten years.

Fig. 9 illustrates the number of proposed ACO routing papers during different periods in time. Before 2005 there were only a few proposed protocols, therefore we summarize them in one time span. From 2005 on, we show the number of papers over four year periods for each category. It can be seen that most of the publications are focused on basic ACO based protocols in MANETs before 2008. After 2010 there is no further study in this category. Since 2007 the three new research directions of energy aware, location aware and security aware ACO based routing protocols have attracted more and more researchers. Therefore, designing routing protocols which aim only for finding the optimal routes was no longer the focus of this research area. While in the period from 2005 to 2008 there was no new QoS aware ACO based routing protocol, this field continues to be actively studied up to now. We infer that QoS will always need to be improved as

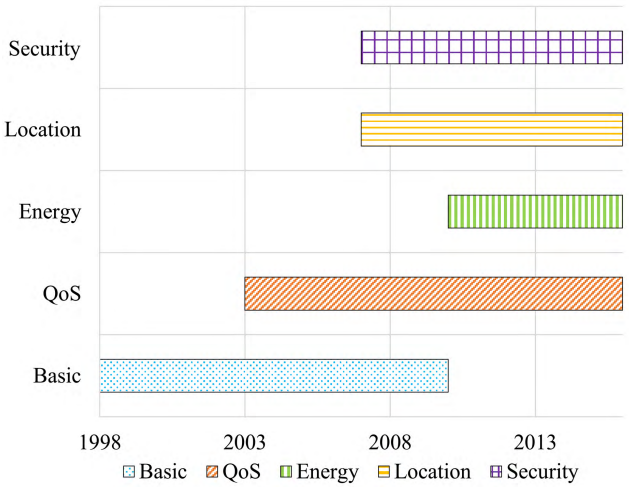


FIGURE 8. The development of ACO based routing protocols.

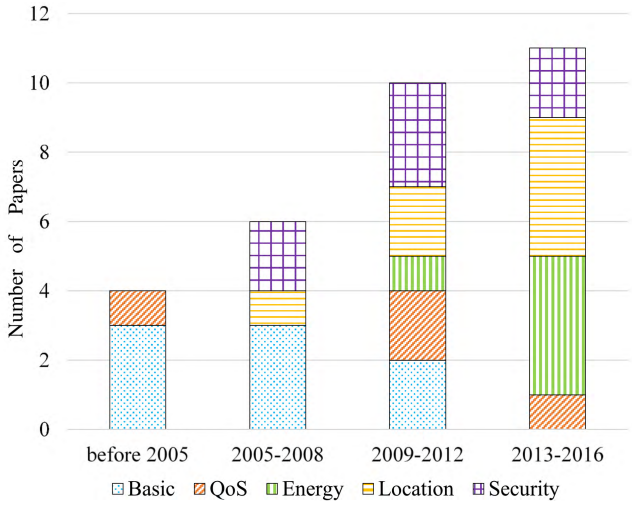


FIGURE 9. The proportion of ACO based routing protocols.

it remains a priority to satisfy users' communication requirements. In recent years, energy efficiency is becoming an independent and significant issue in designing ACO based routing protocols. In Fig. 9 the number of energy aware ACO based protocols rises up significantly after 2009, from 10% of all protocols in the third time slot to 36% in the fourth time slot. However, some of the energy aware protocols make trade-offs with respect to path length or route delay. Further research in this area is still necessary to resolve these open issues.

During the last ten years, location information aware vehicle routing is becoming a hot topic, due to the increasing ubiquity of GPS. Location information aware routing protocols have been widely used, especially in VANETs. From the reviewed ACO based routing protocols in VANETs, we have recognized that most of the protocols are designed for V2V networks. As the V2I communication networks develop progressively, we assume that in the future new protocols

will be proposed in this area. Moreover, since most of the reviewed protocols do not consider any security issues, we infer that designing security and location aware ACO routing protocols in MANETs, would be an interesting future research direction. S-AMCQ [61] is a good example. At the same time, security aware protocols themselves are also a growing field. The proportion of this category remains stable. New protocols in this category are needed to reduce overhead and delay introduced by the security mechanisms, such as authentication processes. Moreover, combining security and other metrics would be valuable. For example, security and energy aware ACO based routing protocols that avoid repeated usage of the optimal secure path could be designed and studied. Combining security and location aware ACO routing protocols for usage in VANETs also seems promising. All in all, designing QoS, energy, location and security aware ACO routing protocol are four main research directions. There are still open questions in each direction which encourage researchers to study further. However, considering multiple issues in the design of a routing protocol can make the protocol more suitable for real world applications. Therefore, we infer that designing ACO routing protocols based on the multiple existing issues in MANETs and especially in VANETs, would be an interesting future research direction.

VI. CONCLUSION

Due to the self-organizing properties of MANETs, routing is considered a challenging problem. The ACO meta-heuristic which presents a common framework for approximating solutions to NP-hard optimization problems is especially applicable to dynamic problems, such as routing in MANETs. In the past two decades, researchers have designed various ACO based routing protocols in MANETs. In this work, we have studied these protocols which have been proposed from 1998 up to now. We have sorted the approaches into five main categories and have briefly reviewed each selected protocol. We have also presented a detailed comparative analysis in terms of protocol design and simulation related parameters for all reviewed protocols. Besides our reviews and our comparisons, we have also discussed the open issues of the surveyed protocols. Additionally, based on our observations, we have summarized the changes in research interests over the years and pointed out promising future directions for research in ACO based routing protocols. The main goal of this work is to give a general overview of the existing ACO based routing protocols for MANETs and we hope this work can encourage protocol designers to take into account the various protocol properties studied so far when designing new ACO based routing protocols.

ACKNOWLEDGMENT

The authors would like to thank Arne Bochem for his invaluable support and suggestions, which have greatly improved this paper. The authors also would like to thank Lars Runge, Milad Ayoub and the reviewers for their helpful comments.

REFERENCES

[1] C. E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 24, no. 4, pp. 234–244, 1994.

[2] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (AODV) routing," IETF, Fremont, CA, USA, Tech. Rep. rfc3561, 2003. Accessed: Oct. 26, 2017. [Online]. Available: https://tools.ietf.org/html/rfc3561

[3] D. B. Johnson *et al.*, "DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks," *Ad hoc Netw.*, vol. 5, pp. 139–172, Jan. 2001.

[4] F. Dressler and O. B. Akan, "A survey on bio-inspired networking," *Comput. Netw.*, vol. 54, no. 6, pp. 881–900, 2010.

[5] G. Beni and J. Wang, "Swarm intelligence in cellular robotic systems," in *Robots Biological Systems: Towards a New Bionics?*. Berlin, Germany: Springer, 1993, pp. 703–712, doi: https://doi.org/10.1007/978-3-642-58069-7_38.

[6] A. K. Kordon, "Swarm intelligence: The benefits of swarms," in *Applying Computational Intelligence*. Berlin, Germany: Springer, 2010, pp. 145–174, doi: https://doi.org/10.1007/978-3-540-69913-2_6.

[7] E. Bonabeau, M. Dorigo, and G. Theraulaz, *Swarm Intelligence: From Natural to Artificial Systems*. Oxford, U.K.: Oxford Univ. Press, 1999.

[8] J. Bishop, "Stochastic searching networks," in *Proc. 1st IEE Int. Conf. Artif. Neural Netw. (Conf.)*, 1989, pp. 329–331.

[9] R. Poli, J. Kennedy, and T. Blackwell, "Particle swarm optimization," *Swarm Intell.*, vol. 1, no. 1, pp. 33–57, Jun. 2007, doi: https://doi.org/10.1007/s11721-007-0002-0.

[10] M. Dorigo, "Optimization, learning and natural algorithms," Ph.D. dissertation, Politecnico di Milano, Milan, Italy, 1992.

[11] H. Zhang, X. Wang, and D. Hogrefe, "A survey of location aware ant colony optimization routing protocols in MANETs," in *Proc. 10th EAI Int. Conf. Bio-Inspired Inf. Commun. Technol. (BIONETICS)*, 2017. [Online]. Available: http://bionetics.org/2017/show/accepted-papers

[12] C. S. Moreau, C. D. Bell, R. Vila, S. B. Archibald, and N. E. Pierce, "Phylogeny of the ants: Diversification in the age of angiosperms," *Science*, vol. 312, no. 5770, pp. 101–104, 2006.

[13] B. Hölldobler and E. O. Wilson, *The ANTS*. Cambridge, MA, USA: Harvard Univ. Press, 1990.

[14] G. F. Oster and E. O. Wilson, *Caste and Ecology in the Social Insects*. Princeton, NJ, USA: Princeton Univ. Press, 1978.

[15] T. Flannery, *Here on Earth: A Natural History of the Planet*. New York, NY, USA: Grove, 2011.

[16] C. Anderson, G. Theraulaz, and J.-L. Deneubourg, "Self-assemblages in insect societies," *Insectes Sociaux*, vol. 49, no. 2, pp. 99–110, 2002.

[17] N. J. Mlot, C. A. Tovey, and D. L. Hu, "Fire ants self-assemble into waterproof rafts to survive floods," *Proc. Nat. Acad. Sci. USA*, vol. 108, no. 19, pp. 7669–7673, 2011.

[18] P. C. Foster, N. J. Mlot, A. Lin, and D. L. Hu, "Fire ants actively control spacing and orientation within self-assemblages," *J. Experim. Biol.*, vol. 217, no. 12, pp. 2089–2100, 2014.

[19] N. Fujiwara-Tsujii, N. Yamagata, T. Takeda, M. Mizunami, and R. Yamaoka, "Behavioral responses to the alarm pheromone of the ant *camponotus obscuripes* (hymenoptera: Formicidae)," *Zool. Sci.*, vol. 23, no. 4, pp. 353–358, 2006.

[20] H. Ahmed and J. Glasgow, "Swarm intelligence: Concepts, models and applications," School Comput., Queens Univ., Kingston, ON, Canada, Tech. Rep. 2012-585, 2012.

[21] F. Moyson and B. Manderick, *The Collective Behavior of Ants: An Example of Self-organization in Massive Parallelism*, Vrije Univ. Brussel, Ixelles, Belgium, 1988.

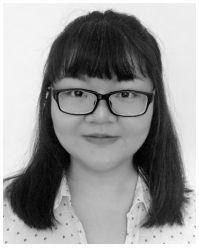
[22] S. Goss, S. Aron, J.-L. Deneubourg, and J. M. Pasteels, "Self-organized shortcuts in the Argentine ant," *Naturwissenschaften*, vol. 76, no. 12, pp. 579–581, 1989.

[23] M. Dorigo and L. M. Gambardella, "Ant colony system: A cooperative learning approach to the traveling salesman problem," *IEEE Trans. Evol. Comput.*, vol. 1, no. 1, pp. 53–66, Apr. 1997.

[24] B. Bullnheimer, R. F. Hartl, and C. Strauß, "A new rank based version of the ant system—A computational study," *Central Eur. J. Oper. Res. Econ.*, vol. 7, pp. 25–38, 1997. Accessed: Oct. 26, 2017. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.49.4735
[25] V. Maniezzo, "Exact and approximate nondeterministic tree-search procedures for the quadratic assignment problem," *INFORMS J. Comput.*, vol. 11, no. 4, pp. 358–369, 1999.
[26] T. Stützle and H. H. Hoos, "MAX–MIN ant system," *Future Generat. Comput. Syst.*, vol. 16, no. 8, pp. 889–914, 2000.
[27] C. Blum and M. Dorigo, "The hyper-cube framework for ant colony optimization," *IEEE Trans. Syst., Man, Cybern. B, Cybern.*, vol. 34, no. 2, pp. 1161–1172, Apr. 2004.
[28] M. Dorigo and T. Stützle, *Ant Colony Optimization*. Cambridge, MA, USA: MIT Press, 2004.
[29] D. W. Corne, A. Reynolds, and E. Bonabeau, "Swarm intelligence," in *Handbook Natural Computing*. Berlin, Germany: Springer, 2012, pp. 1599–1622, doi: 10.1007/978-3-540-92910-9_48.
[30] G. Di Caro and M. Dorigo, "AntNet: Distributed stigmergetic control for communications networks," *J. Artif. Intell. Res.*, vol. 9, pp. 317–365, Dec. 1998.
[31] M. Gunes, U. Sorges, and I. Bouazizi, "ARA-the ant-colony based routing algorithm for MANETs," in *Proc. Int. Conf. Parallel Process. Workshops*, 2002, pp. 79–85.
[32] J. S. Baras and H. Mehta, "A probabilistic emergent routing algorithm for mobile ad hoc networks," in *Proc. Modeling Optim. Mobile, Ad Hoc Wireless Netw. (WiOpt)*, 2003, p. 10.
[33] G. Di Caro, F. Ducatelle, and L. M. Gambardella, "AntHocNet: An adaptive nature-inspired algorithm for routing in mobile ad hoc networks," *Eur. Trans. Telecommun.*, vol. 16, no. 5, pp. 443–455, 2005.
[34] *QualNet 5.2.0 Programmer's Guide*, SCALABLE Netw. Technol., Inc, Culver, CA, USA, 2011.
[35] E. Osagie, P. Thulasiraman, and R. K. Thulasiram, "PACONET: Improved ant colony optimization routing algorithm for mobile ad hoc networks," in *Proc. 22nd Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, 2008, pp. 204–211.
[36] W.-J. Yu, G.-M. Zuo, and Q.-Q. Li, "Ant colony optimization for routing in mobile ad hoc networks," in *Proc. Int. Conf. Mach. Learn.*, vol. 2. 2008, pp. 1147–1151.
[37] J. Wang, E. Osagie, P. Thulasiraman, and R. K. Thulasiram, "HOPNET: A hybrid ant colony optimization routing algorithm for mobile ad hoc network," *Ad Hoc Netw.*, vol. 7, no. 4, pp. 690–705, 2009.
[38] A. Kathirvel, *Introduction to GloMoSim*. Saarbrücken, Germany: LAP Lambert Academic Publishing, 2011.
[39] Z. J. Haas, M. R. Pearlman, and P. Samar, "The zone routing protocol (ZRP) for ad hoc networks," IETF, Fremont, CA, USA, Tech. Rep. draft-ietf-manet-zone-zrp-04, 2002. Accessed: Oct. 26, 2017. [Online]. Available: https://tools.ietf.org/html/draft-ietf-manet-zone-zrp-04
[40] S. Sethi and S. K. Udgata, "The efficient ant routing protocol for MANET," *Int. J. Comput. Sci. Eng.*, vol. 2, no. 7, pp. 2414–2420, 2010.
[41] I. Park, J. Kim, and I. Pu, "Blocking expanding ring search algorithm for efficient energy consumption in mobile ad hoc networks," in *Proc. 3rd Annu. Conf. Wireless On-Demand Netw. Syst. Services (WONS)*, 2006, pp. 191–195.
[42] O. Hussein and T. Saadawi, "Ant routing algorithm for mobile ad-hoc networks (ARAMA)," in *Proc. IEEE Int. Perform., Comput., Commun. Conf.*, Apr. 2003, pp. 281–290.
[43] E. Khosrowshahi-Asl, M. Noorhosseini, and A. S. Pirouz, "A dynamic ant colony based routing algorithm for mobile ad-hoc networks," *J. Inf. Sci. Eng.*, vol. 27, no. 5, pp. 1581–1596, 2011.
[44] P. V. Krishna, V. Saritha, G. Vedha, A. Bhiwal, and A. S. Chawla, "Quality-of-service-enabled ant colony-based multipath routing for mobile ad hoc networks," *IET Commun.*, vol. 6, no. 1, pp. 76–83, 2012.
[45] A. D. Al-Ani and J. Seitz, "QoS-aware routing in multi-rate ad hoc networks based on ant colony optimization," *Netw. Protocols Algorithms*, vol. 7, no. 4, pp. 1–25, 2016.
[46] J. D. Case, M. Fedor, M. L. Schoffstall, and J. Davin, "Simple network management protocol (SNMP)," IETF, Fremont, CA, USA, Tech. Rep. rfc1157, 1990. [Online]. Available: http://www.rfc-editor.org/info/rfc1157
[47] T. Back, *Evolutionary Algorithms in Theory and Practice: Evolution Strategies, Evolutionary Programming, Genetic Algorithms*. Oxford, U.K.: Oxford Univ. Press, 1996.
[48] I. Woungang, M. S. Obaidat, S. K. Dhurandher, A. Ferworn, and W. Shah, "An ant-swarm inspired energy-efficient ad hoc on-demand routing protocol for mobile ad hoc networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jul. 2013, pp. 3645–3649.
[49] S. Misra, S. K. Dhurandher, M. S. Obaidat, P. Gupta, K. Verma, and P. Narula, "An ant swarm-inspired energy-aware routing protocol for wireless ad-hoc networks," *J. Syst. Softw.*, vol. 83, no. 11, pp. 2188–2199, 2010.
[50] P. Vijayalakshmi, S. A. J. Francis, and J. A. Dinakaran, "A robust energy efficient ant colony optimization routing algorithm for multi-hop ad hoc networks in MANETs," *Wireless Netw.*, vol. 22, no. 6, pp. 1–20, 2015.
[51] J. Zhou, H. Tan, Y. Deng, L. Cui, and D. D. Liu, "Ant colony-based energy control routing protocol for mobile ad hoc networks under different node mobility models," *EURASIP J. Wireless Commun. Netw.*, vol. 2016, no. 1, p. 105, Dec. 2016, doi: https://doi.org/10.1186/s13638-016-0600-x.
[52] S. B. Prabaharan and R. Ponnusamy, "Secure and energy efficient MANET routing incorporating trust values using hybrid ACO," in *Proc. Int. Conf. Comput. Commun. Informat. (ICCCI)*, 2016, pp. 1–8.
[53] P. Misra and P. Enge, *Global Positioning System: Signals, Measurements and Performance*, 2nd ed. Lincoln, MA, USA: Ganga-Jamuna Press, 2006.
[54] S. Kamali and J. Opatrny, "POSANT: A position based ant colony routing algorithm for mobile ad-hoc networks," in *Proc. 3rd Int. Conf. Wireless Mobile Commun. (ICWMC)*, 2007, p. 21.
[55] D. Kadono, T. Izumi, F. Ooshita, H. Kakugawa, and T. Masuzawa, "An ant colony optimization routing based on robustness for ad hoc networks with GPSs," *Ad Hoc Netw.*, vol. 8, no. 1, pp. 63–76, 2010.
[56] S. L. O. B. Correia, J. Celestino, and O. Cherkaoui, "Mobility-aware ant colony optimization routing for vehicular ad hoc networks," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Mar. 2011, pp. 1125–1130.
[57] M. Killat and H. Hartenstein, "An empirical model for probability of packet reception in vehicular ad hoc networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, no. 1, p. 721301, Dec. 2009, doi: https://doi.org/10.1155/2009/721301.
[58] J. Härri, C. Bonnet, and F. Filali, "Kinetic mobility management applied to vehicular ad hoc network protocols," *Comput. Commun.*, vol. 31, no. 12, pp. 2907–2924, 2008.
[59] H. Rana, P. Thulasiraman, and R. K. Thulasiram, "MAZACORNET: Mobility aware zone based ant colony optimization routing for VANET," in *Proc. IEEE Congr. Evol. Comput.*, Jun. 2013, pp. 2948–2955.
[60] S. Balaji, S. Sureshkumar, and G. Saravanan, "Cluster based ant colony optimization routing for vehicular ad hoc networks," *Int. J. Sci. Eng. Res.*, vol. 4, no. 6, pp. 26–30, Jun. 2013.
[61] M. H. Eiza, T. Owens, and Q. Ni, "Secure and robust multi-constrained QoS aware routing algorithm for VANETs," *IEEE Trans. Depend. Sec. Comput.*, vol. 13, no. 1, pp. 32–45, Jan. 2016.
[62] V. Vijayalakshmi and T. Palanivelu, "Secure antnet routing algorithm for scalable adhoc networks using elliptic curve cryptography," *J. Comput. Sci.*, vol. 3, no. 12, pp. 939–943, 2007.
[63] V. Kapoor, V. S. Abraham, and R. Singh, "Elliptic curve cryptography," *Ubiquity*, vol. 2008, no. 5, pp. 7:1–7:8, May 2008, doi: 10.1145/1378355.1378356.
[64] S. Mehfuz and M. N. Doja, "Swarm intelligent power-aware detection of unauthorized and compromised nodes in MANETs," *J. Artif. Evolution Appl.*, vol. 2008, Nov. 2008, Art. no. 236803. [Online]. Available: http://dx.doi.org/10.1155/2008/236803
[65] H. Krawczyk, R. Canetti, and M. Bellare, "HMAC: Keyed-hashing for message authentication," IETF, Fremont, CA, USA, Tech. Rep. rfc2104, 1997. [Online]. Available: https://tools.ietf.org/html/rfc2104
[66] P. Papadimitratos and Z. J. Haas, "Secure routing for mobile ad hoc networks," in *Proc. SCS Commun. Netw. Distrib. Syst. Modeling Simulation Conf. (CNDS)*, San Antonio, TX, USA, Jan. 2002, pp. 193–204.
[67] S. J. Mirabedini and M. Teshnehlab, "FuzzyAntNet: A novel multi-agent routing algorithm for communications networks," *Comput. Sci. Telecommun.*, vol. 12, no. 1, pp. 45–49, 2007.
[68] S. J. Mirabedini, M. Teshnehlab, and A. Rahmani, "FLAR: An adaptive fuzzy routing algorithm for communications networks using mobile ants," in *Proc. Int. Conf. Converg. Inf. Technol.*, 2007, pp. 1308–1315.

[69] S. J. Mirabedini, M. Teshnehlab, M. Shenasa, A. Movaghar, and A. M. Rahmani, "AFAR: Adaptive fuzzy ant-based routing for communication networks," *J. Zhejiang Univ. Sci. A*, vol. 9, no. 12, pp. 1666–1675, 2008.
[70] M. Goswami, R. Dharaskar, and V. Thakare, "Fuzzy ant colony based routing protocol for mobile ad hoc network," in *Proc. Int. Conf. Comput. Eng. Technol. (ICCET)*, vol. 2. 2009, pp. 438–444.
[71] S. Sethi and S. K. Udgata, "Fuzzy-based trusted ant routing (FTAR) protocol in mobile ad hoc networks," in *Proc. Int. Workshop Multi-Disciplinary Trends Artif. Intell.*, 2011, pp. 112–123.
[72] G. Indirani and K. Selvakumar, "Swarm based detection and defense technique for malicious attacks in mobile ad hoc networks," *Int. J. Comput. Appl.*, vol. 50, no. 19, pp. 1–6, 2012.
[73] K. Sowmya, T. Rakesh, and D. P. Hudedagaddi, "Detection and prevention of blackhole attack in MANET using ACO," *Int. J. Comput. Sci. Netw. Secur.*, vol. 12, no. 5, p. 21, 2012.
[74] S. Pal, K. Ramachandran, I. D. Paul, and S. Dhanasekaran, "A review on anomaly detection in manet using antnet algorithm," *Middle-East J. Sci. Res.*, vol. 22, no. 5, pp. 690–697, 2014.
[75] P. Memarmoshrefi, H. Zhang, and D. Hogrefe, "Investigation of a bio-inspired security mechanism in mobile ad hoc networks," in *Proc. WiMob*, 2013, pp. 709–716.
[76] P. Memarmoshrefi, H. Zhang, and D. Hogrefe, "Social insect-based sybil attack detection in mobile ad-hoc networks," in *Proc. 8th Int. Conf. Bioinspired Inf. Commun. Technol.*, 2014, pp. 141–148.
[77] H. Zhang, P. Memarmoshrefi, F. Ashrafi, and D. Hogrefe, "Investigating the learning phase of an autonomous authentication in mobile ad-hoc networks," in *Proc. 9th EAI Int. Conf. Bio-Inspired Inf. Commun. Technol. (BIONETICS)*, 2016, pp. 91–92.
[78] T. Issariyakul and E. Hossain, *Introduction to Network Simulator NS2*. Springer, 2011.
[79] Riverbed Technology, San Francisco, CA, USA. *Opnet Simulator*. Accessed: Oct. 18, 2017. [Online]. Available: https://www.riverbed.com/de/products/steelcentral/opnet.html?redirect=opnet
[80] A. Varga *et al.*, "The OMNeT++ discrete event simulation system," in *Proc. Eur. Simulation Multi Conf. (ESM)*, vol. 9. 2001, p. 65.
[81] G. Carneiro, "NS-3: Network simulator 3," in *Proc. UTM Lab Meeting*, Apr. 2010, p. 20.
[82] J. Nzouonta. *Vehicular Network Movement Generator*. Accessed: Jan. 1, 2011. [Online]. Available:http://web.njit.edu/~borcea/invent/
[83] S. M. Mousavi, H. R. Rabiee, M. Moshref, and A. Dabirmoghaddam, "Mobisim: A framework for simulation of mobility models in mobile ad-hoc networks," in *Proc. 3rd IEEE Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, Oct. 2007, p. 82.
[84] M. Liu, Y. Sun, R. Liu, and X. Huang, "An improved ant colony QoS routing algorithm applied to mobile ad hoc networks," in *Proc. Int. Conf. Wireless Commun., Netw. Mobile Comput.*, Sep. 2007, pp. 1641–1644.
[85] R. Barr. (Mar. 2004). *Swans-Scalable Wireless Ad Hoc Network Simulator*. [Online]. Available: http://jist.ece.cornell.edu/docs.html

HANG ZHANG received the B.S. degree in information and computer science from the Changsha University of Science and Technology in 2005 and the M.S. degree in computer science from the Georg-August-University of Goettingen in 2012. Her research interests include designing secure communication protocols in wireless mobile ad hoc and vehicle ad hoc networks by applying bio-inspired algorithms. Her current research interests include applying ant colony optimization algorithm and fuzzy logic to ensure secure routing in wireless networks.



XI WANG received the B.S. degree in network engineering from Tianjin Polytechnic University in 2014. She is currently pursuing the M.S. degree in Internet technologies and information system with the Georg-August-University of Goettingen. Her research interests include self-organizing networks, authentication mechanisms, and the communication in vehicle ad hoc networks.

PARISA MEMARMOSHREFI is currently a Research Staff Member with the Telematics Group, Institute of Computer Science, Georg-August-University of Goettingen. Her research area is security in self-organizing and distributed systems, such as wireless ad hoc and sensor networks. Among security provision mechanisms, her current research interests include bio-inspired wireless network security. She is also interested in autonomous authentication and soft security mechanisms (trust-based systems).

DIETER HOGREFE received the degree from the Philips Exeter Academy, USA, in 1976, and the Ph.D. degree in computer science and mathematics from the University of Hannover, Germany, in 1985. From 1983 to 1986, he was with the SIEMENS Research Center, Munich, and was involved in the analysis of telecommunication systems. He was responsible for the protocol simulation and analysis of the CCS No. 7. From 1996 to 2010, he was the Chairman of the Technical Committee Methods for Testing and Specification at the European Telecommunication Standards Institute, ETSI. Since 2002, he has been a Full Professor (C4) of telematics with the Georg-August-University of Goettingen. Since 2003, he has been the Director of the Institute of Computer Science. From 2011 to 2013, he was the Dean of the Faculty of Mathematics and Computer Science. He held a full professor positions at the Universities of Bern, Luebeck, and Goettingen and visiting positions at the University of Dortmund, Technical University Budapest, UC Berkeley, and Hamilton University. He published numerous papers and two books on Internet technology, security of wireless sensor networks, and analysis, simulation, and testing of formally specified communication systems. His research activities are directed toward computer networks and communication software engineering.

His research interests include the development of new communication protocols, in particular for the support of signaling services, that enhance security, quality, and configurability of Internet connections in general and in the mobile context in particular; methodology for development of new protocols, in particular or specification, implementation and testing; economic and legal issues arising from new and enhanced communication services over the Internet, in particular in the mobile context.