International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-4, November 2019

Trust based Secure and Energy Efficient Routing using ACO for WSN

A.Jainulabudeen, M.Mohamed Surputheen

Abstract: ***Secure and energy efficient routing is one of the major requirements of the WSN models. This is due to the resource constrained environments and remotely deployed conditions. This work proposes an effective model that ensures security and energy efficiency during the routing process in a WSN. The proposed model modifies the Ant Colony Optimization algorithm to perform routing based on these multiple objectives. The proposed model uses trust as the major component to provide security, and the randomness associated with the metaheuristic nature of the model enables uniform usage of all sensor nodes. This also extends the network lifetime, making the proposed model highly efficient and deployable in real-time networks. Experiments and comparisons also indicate that the proposed model exhibits shorter time requirements and provides more optimized paths compared to models in literature.***

Keywords: Wireless Sensor Networks, Routing, TRMA Model, Security, ACO.

I. INTRODUCTION

The huge adoption of networks and network based processes in the recent years has resulted in a large number of Wireless Sensor Networks (WSN) to be employed in several areas [1,2]. One major challenge in using a WSN model is the adoption of an effective routing mechanism to provide secure transmission of data [3]. The challenges arise from the nature of the network and the network nodes. Nodes in WSN are generally sensors and power constrained. Further, they are usually deployed in remote locations, hence possibility of physical attacks is high [4,5]. The routing mechanism should consider all these issues while selecting transmission routes.

Several routing mechanisms have been put forth to provide safe and effective routing. The mechanisms can be divided into three broad categories; proactive, reactive and hybrid. Proactive routing models stores the routes and uses them as and when required, while reactive routing models determine routes based on the transmission requirements. Proactive routing works effectively on static environments, while dynamic environments require reactive routing models. Hybrid routing is a combination of both proactive and reactive models [6]. Efficient routing in WSN requires more than just effective routing. Trust and energy efficiency play a vital role in the routing model apart from the transmission distance. Credibility of a node is a mandatory aspect to identify if the node is malicious or under attack [7]. Energy efficiency is defined by moderate power depletion in nodes. Hence a routing model deigned for WSN should consider trust levels and energy efficiency apart from the usual distance measure. This makes routing a multi-objective decision-making problem. This work proposes a modified Ant Colony Optimization (ACO) based routing model, that includes trust as a major component in its objective function. The significance of trust and distance are defined during the selection of nodes and the final route selection process uses the multi criteria objective function to determine the best route. The remainder of this work is presented as follows: Section II presents a review of literature, Section III presents a detailed description of the working of the proposed model, Section IV presents the results and discussion and Section V concludes the work.

Manuscript published on November 30, 2019.
* Correspondence Author
A.Jainulabudeen*, Research Scholar, Department of Computer Science, Jamal Mohamed College (Autonomous), (Affiliated to Bharathidasan University), Tiruhcirappalli, Tamilnadu, India.
Dr. M.Mohamed Surputheen, Associate Professor, Department of Computer Science, Jamal Mohamed College (Autonomous), (Affiliated to Bharathidasan University), Tiruchirappalli, Tamilnadu, India.

II. LITERATURE REVIEW

Secure routing plays a significant role in determining the efficiency of a WSN. Several contributions in terms of routing models are available in this domain. Some important contributions are discussed in this section.

A secure and on-demand routing model was proposed by Upendran et al. [8]. This work uses Particle Swarm Optimization (PSO) as the route generation mechanism. The node selection is performed only on-demand. Hence every node in the path is selected in random, making the model secure. An ACO based routing model for secure routing was proposed by Sun et al. [9]. The model proposes to achieve security with lowered energy consumption. The model uses Pareto modelling to obtain the final solution. An analysis of metaheuristic modelling and the generic nature of the modelling mechanism was proposed by Prakasam et al. [10]. This work exhibits the generic and fine tunable nature of ACO models to incorporate additional objective criterion. The model deals with routing, however, is not specific to WSN routing. A fuzzy logic based ACO model for routing in Vehicular Adhoc NETworks (VANET) is proposed by Fatemidokht et al. [11]. This technique uses a combination of ACO and Fuzzy logic for routing. Other works using ACO includes model by Junnarkar et al. [12] dealing with QoS and Mobility Aware models. These models however do not deal with the security aspect from the point of trust levels of nodes.

Trust levels play a significant role in the routing process. A secure routing model that considers trust as the main aspect for routing was proposed by Yang et al. [13]. This work proposes an energy optimized routing model Energy-optimized Secure Routing (EOSR), which also provides secure transmissions. The trust levels are used to identify malicious nodes. A clustering based model that uses trust factors for routing was proposed by Gaber et al. [14]. This work uses the Bat Optimization Algorithm for identifying the cluster heads. The cluster heads aid in secure routing. Other trust based models that uses clustering mechanisms for secure routing are models by Ganesh et al. [15] and Lu et al. [16].

An adaptive model for energy efficient routing was proposed by Singh et al. [17]. This is also a clustering based model and uses weighted probability levels to identify the cluster heads. The model also uses cross layer mechanisms to achieve high QoS. A random routing model that protects the source location in the routing process was proposed by He et al. [18]. This model has also been extended for Internet of Things domain. This is sector based random routing model that reduces energy consumption during the routing process. The model uses phantom nodes to hide the source location. Other models dealing with source location privacy are by Huang et al. [19], Yang et al. [20] and Han et al. [21].

III. NETWORK MODEL

The key points of the network model are as follows

- The network is composed of a large and defined number of sensor nodes.
- Each node is constrained by the computing power and energy source.
- It is also assumed that once deployed, the location of these sensors does not change.
- A powerful sink node whose location is defined and is public in the network.
- An event based reactive routing mechanism is assumed within the network.
- The events are also assumed to be raised in random and by any node in the network.

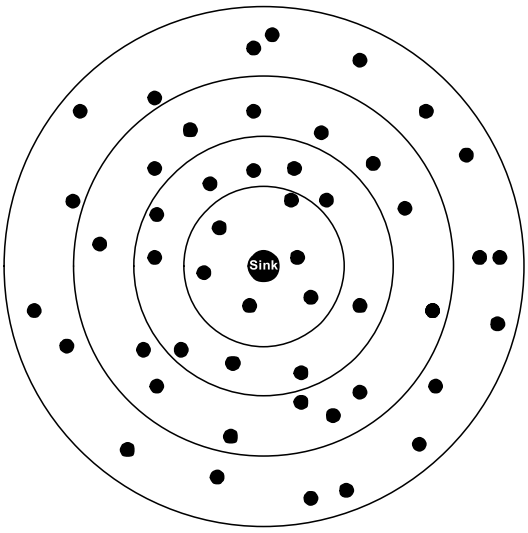

Fig. 1.WSN Network Model

IV. TRUST BASED ROUTING USING MODIFIED ACO (TRMA)

Routing in WSN (Fig 1) requires the identification of secure nodes in the network, through which the packet transmission can take place. Routing is always expected to be secure such that the mode of transmission can reduce loss due to attacks to a large extent. However, this functionality always comes with increase in energy consumption, as nodes in the network must perform additional computations to obtain the secure node. Increase in energy consumption often leads to a reduction in the network lifetime. Sensors in the networks are usually battery operated and hence they are highly resource constrained. Battery depletion in sensors often lead to dead nodes. This in turn results in the degradation of the networks, hence reducing the network lifetime. Security vs. computation is always a tradeoff during the process of routing. Models proposed for routing are expected to achieve the best balance between energy consumption and security. This work provides a modified ACO based routing mechanism that provides compute effective and secure transmissions.

A. Search Space Creation and Parameter Initialization

ACO [22] operates on a defined and a static search space. The network containing sensors constitutes the search space for ACO. Every sensor and the connections between these sensors are recorded to form a graph. ACO performs traversals on this graph to determine the routing paths [23]. Sensors form nodes and connections between them constitute the edges. Sensors in WSN do not have direct connections between them. Instead, sensors that are within the communication radius of a node are considered to be connected to it. Hence the communication radius determines the presence or absence of edges between the nodes.

Every sensor is in the network is composed of several attributes. The routing process mainly uses the distance factors and the trust levels of nodes. During deployment, all nodes are given equal trust levels. As communication progresses, the trust values are modified to reflect the trust status of sensor.

ACO based parameters are mapped to these existing attributes of the sensor nodes for effective routing. ACO based properties include; number of ants (m), significance of trail intensity (α), significance of distance between nodes (β), evaporation coefficient (ρ) and level of pheromone to be deposited after every transmission (Q). Trail intensity between nodes (τ) is mapped to trust levels of the sensor network. Higher trail between nodes defines higher trust and low trail levels define lower trust. Evaporation coefficient aids in the deterioration of trust levels of a node. Every successful transmission increases the trail intensity levels. However, failure in transmission cannot be directly detected. Employing techniques for detecting failed transmissions will result in loss of computational resources. Hence if no traffic was observed between sensors, the trust levels automatically start to degrade. Successful transmission of packets increases the trust levels by Q. Hence attacked nodes automatically

lose their trust levels. Parameter values used by this work is shown in Table I.

Table- I: Parameters used by TRMA

Parameters	Value
A	0.5
B	0.3
P	0.1
M	10
Q	0.8
Initial Trust	1

Initialization of parameters and construction of the network graph forms first phase of the processing model.

B. Trust based Objective Function

The objective function in a metaheuristic model is used to determine the fitness of a solution. The objective function of ACO is the probability function that determines the fitness of a solution. ACO uses a combination of trail intensity and distance in its objective function. The fitness of a node *j* from a node *i* is given by

$$p_{ij}(t) = \frac{[\tau_{ij}(t)]^{\alpha}.[\eta_{ij}]^{\beta}}{\sum_{j=1}^{n}[\tau_{ij}(t)]^{\alpha}.[\eta_{ij}]^{\beta}}$$

Where τ_{ij} is the pheromone trail between sensors *i* and *j*, and η_{ij} is the distance between the sensors.η_{ij} is determined by

$$\eta_{ij} = \frac{1}{\sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}}$$

The proposed modified ACO model updates this objective function by incorporating the trust levels. This makes trust play a vital role in the node selection process. Trust is of three types; direct trust, indirect trust and comprehensive trust.

Direct trust is the trust level between two specific nodes *i* and *j*. It is given by

$$DT_{ij} = \frac{c_{ij} + 1}{c_{ij} + nc_{ij} + 2}$$

Where c_{ij} is the number of cooperative interactions between *i* and *j* and nc_{ij} is the number of non-cooperative interactions between *i* and *j*.

It is not sufficient to analyze the interactions between two nodes alone to determine the trust levels. Hence indirect trust is calculated. Indirect trust uses trust levels of an intermediate node to determine the trust levels of a node. Indirect trust is given by

$$IT_{ij}^{k} = DT_{ik} + DT_{kj}$$

The direct and the indirect trust levels are combined together to form the comprehensive trust. The comprehensive trust is given by

$$T_{ij} = \mu.DT_{ij} + \frac{1-\mu}{n}\sum_{k=1}^{n} IT_{ij}^{k}$$

Where μ is the weight of direct trust and n is the number of nodes.

The comprehensive trust determines the trail intensity in the proposed modified ACO algorithm.

$$\tau_{ij} = T_{ij}$$

Hence node selection for every iteration is performed based on the trust and the distance measures. The modified objective function is given below

$$p_{ij}(t) = \frac{[T_{ij}(t)]^{\alpha}.[\eta_{ij}]^{\beta}}{\sum_{j=1}^{n}[T_{ij}(t)]^{\alpha}.[\eta_{ij}]^{\beta}}$$

C. Reactive Routing using Modified ACO

Routing is the process of identifying the optimal path for packet transmission. When a request for transmission arises, the packets are created, and a route is determined for each of the packets to be transmitted.

Route determination is performed by the modified ACO. Nodes to be used for routing are determined based on the objective function that uses trust levels and the distance measures. After the selection of each node *j*, and successful transmission of a packet from *i* to *j*, the trust levels between *i* and *j* are modified using the formula,

$$\tau_{ij}(t+1) = \rho.\tau_{ij}(t) + \Delta\tau_{ij}(t, t+1)$$

The value of $\Delta\tau_{ij}$ is given by Q, the trail intensity level to be used for updating. The process is repeated for each ant until the ant reaches the sink node.

At the end of the iteration, every ant contains a path for reaching the sink node. General ACO determines the shortest path and selects it as the best path for traversal. however, the WSN requires not just the shortest path, but also the most secure path. The modified ACO uses a multi objective decision-making mechanism to obtain the best and the secure path. The multi-objective function used to determine the optimal path is given by

$$F_a = \alpha\sum_{i=1}^{p-1} T_{path(i),path(i+1)} + \beta\sum_{i=1}^{p-1}\eta_{path(i),path(i+1)} \quad \forall\, a = 1,2,\dots m$$

Where F_a is the fitness of the path given by ant *a*, *p* is the number of nodes in the path, $T_{path(i),path(i+1)}$ is the trust level between nodes *i* and *i+1* in the path and $\eta_{path(i),path(i+1)}$ is the distance between nodes *i* and *i+1* in the path.

The path exhibiting highest fitness is used as the final path for transmission.

V. RESULTS AND DISCUSSION

The TRMA routing algorithm has been implemented using C#.NET. The network is built using 30 nodes. Each node is assigned with all the properties pertaining to the ACO model and the trust levels. The objective functions were defined and the results were recorded in terms of time, distance covered for a path and the node utility levels. The algorithm was operated in two phases. The first phase identifies a route to traverse the entire network and the second phase identifies a route to travel between specific nodes.

Selection overhead is depicted in figure 2. Selection overhead is the time required to identify the path once a transmission request arises. Low selection overhead represents faster algorithms. It could be observed that the selection overheads exhibit time requirements of ~1.1 second. This is a short time requirement, exhibits the fast processing nature of the proposed model.

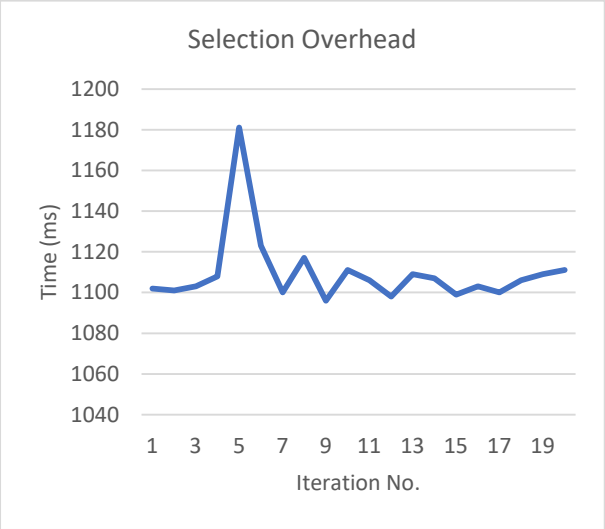

Fig. 2. Selection Overhead

The selection overhead incurred for determining a specific path that traverses between two defined nodes is shown in figure 3. It could be observed that this path exhibits an average requirement of 0.01 second. This exhibits the efficiency of the proposed model.

Comparison is performed with the PSO based routing model proposed by Upendran et al. [8]. The initial comparison is performed based on the distance covered, representing the efficiency of the routing process (Figure 4). Distance covered is proportional to the energy depletion, hence lower the distance covered, better the network lifetime. It could be observed that the proposed TRMA model exhibits lower distance levels compared to the PSO based model proposed by Upendran et al., representing the efficiency of the routing process.

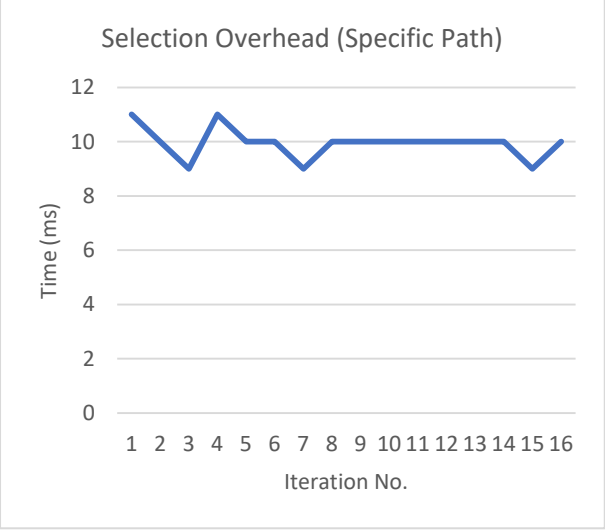

Fig. 3. Specific path based Selection Overhead

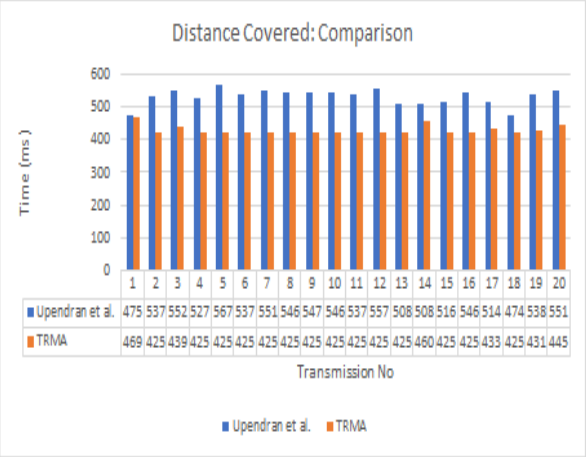

Fig. 4. Comparison of Distance Covered by the Models

A comparison of the node usage levels is shown in figure 5. Usage levels of nodes is a sensor network should be distributed to enable energy efficiency and better network lifetime. It could be observed that the TRMA model exhibits moderate node usage levels and it is consistent on all nodes. Whereas, the model proposed by Upendran et al. utilizes several nodes to a large extent and many nodes are under utilized. This leads to irregular resource depletion, resulting in dead nodes. Hence in terms of node utility, the TRMA model was found to be highly efficient.

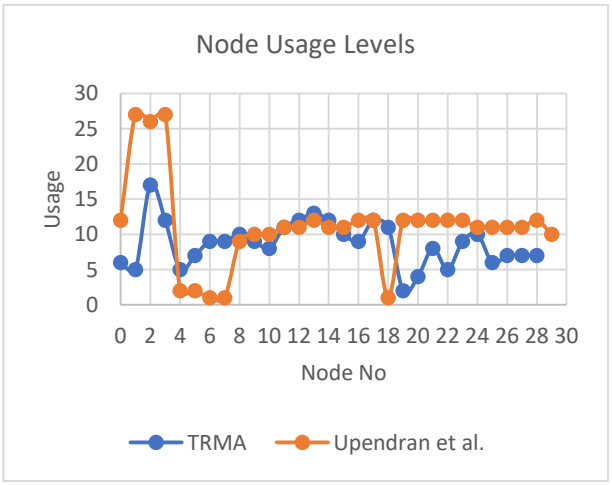

Fig. 5. Comparison of Node Usage Levels

VI. CONCLUSION

Routing in WSN requires the routing model to incorporate security and energy efficiency, due to the constrained nature of WSN environments. This work proposes a secure and energy efficient model to perform routing in WSN. The proposed TRMA model uses modified ACO for the routing process. Trust levels of nodes are identified, and they form the major component of inculcating the security aspect into the model. The routing algorithm is modelled as a multi-criteria decision making problem, which incorporates the trust levels along with the distance factors. Further, the randomized nature of the model enables uniform usage of nodes, resulting in energy efficient routing.

The major limitations of the model is that it is used in static environments. However, the base routing protocol is dynamic in nature. Hence the model can be used in dynamic environment with minimal changes to the working architecture. Incorporating dynamicity into the model can also ensure effective handling of dead nodes in the network, thereby reducing the issues that arise due to dead nodes.

REFERENCES

1. Qiu, Tie, Ruixuan Qiao, and Dapeng Oliver Wu. "EABS: An event-aware backpressure scheduling scheme for emergency Internet of Things." IEEE Transactions on Mobile Computing 17, no. 1 (2017): 72-84.
2. Heinzelman, Wendi Rabiner, Anantha Chandrakasan, and Hari Balakrishnan. "Energy-efficient communication protocol for wireless microsensor networks." In Proceedings of the 33rd annual Hawaii international conference on system sciences, pp. 10-pp. IEEE, 2000.
3. Qiu, Tie, Aoyang Zhao, Ruixin Ma, Victor Chang, Fangbing Liu, and Zhangjie Fu. "A task-efficient sink node based on embedded multi-core soC for Internet of Things." Future Generation Computer Systems 82 (2018): 656-666.
4. Sajjad, Syed Muhammad, Safdar Hussain Bouk, and Muhammad Yousaf. "Neighbor node trust based intrusion detection system for WSN." Procedia Computer Science 63 (2015): 183-188.
5. Han, Guangjie, Xuan Yang, Li Liu, Mohsen Guizani, and Wenbo Zhang. "A disaster management-oriented path planning for mobile anchor node-based localization in wireless sensor networks." IEEE Transactions on Emerging Topics in Computing (2017).
6. Fang, Weidong, Chuanlei Zhang, Zhidong Shi, Qing Zhao, and Lianhai Shan. "BTRES: Beta-based Trust and Reputation Evaluation System for wireless sensor networks." Journal of Network and Computer Applications 59 (2016): 88-94.
7. Sakthidevi, I., and E. Srievidhyajanani. "Secured fuzzy based routing framework for dynamic wireless sensor networks." In 2013 International Conference on Circuits, Power and Computing Technologies (ICCPCT), pp. 1041-1046. IEEE, 2013.
8. Upendran, V., and R. Dhanapal. "Secure and Distributed On-Demand Randomized Routing in WSN." International Journal of Computers & Technology 15, no. 6 (2016): 6850-6856.
9. Sun, Ziwen, Min Wei, Zhiwei Zhang, and Gang Qu. "Secure Routing Protocol based on Multi-objective Ant-colony-optimization for wireless sensor networks." Applied Soft Computing 77 (2019): 366-375.
10. Prakasam, Anandkumar, and Nickolas Savarimuthu. "Metaheuristic algorithms and probabilistic behaviour: a comprehensive analysis of Ant Colony Optimization and its variants." Artificial Intelligence Review 45, no. 1 (2016): 97-130.
11. Fatemidokht, Hamideh, and Marjan Kuchaki Rafsanjani. "F-Ant: an effective routing protocol for ant colony optimization based on fuzzy logic in vehicular ad hoc networks." Neural Computing and Applications 29, no. 11 (2018): 1127-1137.
12. Junnarkar, Aparna, and A. B. Bagwan. "Novel Quality of Service (QOS) Improvement Routing Protocol for MANET Using Ant Colony Optimization." In 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA), pp. 1-6. IEEE, 2017.
13. Yang, Tao, Xu Xiangyang, Li Peng, Li Tonghui, and Pan Leina. "A secure routing of wireless sensor networks based on trust evaluation model." Procedia computer science 131 (2018): 1156-1163.
14. Gaber, Tarek, Sarah Abdelwahab, Mohamed Elhoseny, and Aboul Ella Hassanien. "Trust-based secure clustering in WSN-based intelligent transportation systems." Computer Networks 146 (2018): 151-158.
15. Ganesh, Subramanian, and Ramachandran Amutha. "Efficient and secure routing protocol for wireless sensor networks through SNR based dynamic clustering mechanisms." Journal of Communications and Networks 15, no. 4 (2013): 422-429.
16. Lu, Huang, Jie Li, and Mohsen Guizani. "Secure and efficient data transmission for cluster-based wireless sensor networks." IEEE transactions on parallel and distributed systems 25, no. 3 (2013): 750-761.
17. Singh, Ramnik, and Anil Kumar Verma. "Energy efficient cross layer based adaptive threshold routing protocol for WSN." AEU-International Journal of Electronics and Communications 72 (2017): 166-173.
18. He, Yu, Guangjie Han, Hao Wang, James Adu Ansere, and Whenbo Zhang. "A sector-based random routing scheme for protecting the source location privacy in WSNs for the Internet of Things." Future Generation Computer Systems 96 (2019): 438-448.
19. Huang, Ching-Sheng, Tao Yang, and Hund-Der Yeh. "Review of analytical models to stream depletion induced by pumping: Guide to model selection." Journal of Hydrology 561 (2018): 277-285.
20. Yang, Tao, Tong Cui, Chong-Yu Xu, Philippe Ciais, and Pengfei Shi. "Development of a new IHA method for impact assessment of climate change on flow regime." Global and planetary change 156 (2017): 68-79.
21. Han, Guangjie, Lina Zhou, Hao Wang, Wenbo Zhang, and Sammy Chan. "A source location protection protocol based on dynamic routing in WSNs for the Social Internet of Things." Future Generation Computer Systems 82 (2018): 689-697.
22. Stützle, Thomas, and Marco Dorigo. "ACO algorithms for the traveling salesman problem." Evolutionary algorithms in engineering and computer science (1999): 163-183.
23. Dorigo, Marco, Mark Zlochin, Nicolas Meuleau, and Mauro Birattari. "Updating ACO pheromones using stochastic gradient ascent and cross-entropy methods." In Workshops on Applications of Evolutionary Computation, pp. 21-30. Springer, Berlin, Heidelberg, 2002.