


ITC 3/49 Information Technology and Control Vol. 49 / No. 3 / 2020 pp. 308-319 DOI 10.5755/j01.itc.49.3.25265	Black Hole Attack Prevention in Mobile Ad-hoc Network (MANET) Using Ant Colony Optimization Technique	
	Received 2020/02/10	Accepted after revision 2020/04/25
	 http://dx.doi.org/10.5755/j01.itc.49.3.25265	

HOW TO CITE: Khan, D. M., Aslam, T., Akhtar, N., Qadri, S., Khan, N. A., Rabbani, I. M., Aslam, M. (2020). Black Hole Attack Prevention in Mobile Ad-hoc Network (MANET) Using Ant Colony Optimization Technique. *Information Technology and Control*, 49(3), 308-319. <https://doi.org/10.5755/j01.itc.49.3.25265>

Black Hole Attack Prevention in Mobile Ad-hoc Network (MANET) Using Ant Colony Optimization Technique

Dost Muhammad Khan, Talal Aslam, Nadeem Akhtar, Salman Qadri, Noman Ameer Khan

Department of Computer Science and IT, The Islamia University of Bahawalpur, Pakistan,
 e-mails: khan.dostkhan@iub.edu.pk; mtalalaslaml@gmail.com; nadeem.akhtar.phd@gmail.com;
salman.qadri@iub.edu.pk; nomanameerkhan@gamil.com

Imran Mujaddid Rabbani*, Muhammad Aslam

Dept. of Computer Science, University of Engineering and Technology, Lahore;
 e-mails: irmranmrabbani@gmail.com; maslam@uet.edu.pk

*Corresponding author: imranmrabbani@gmail.com

The Mobile ad-hoc networks are auto configured systems where hubs can travel towards any direction. The hubs do not rely on any external entity to build the framework. Because of its versatility, the black hole is a real security issue to be settled. It occurs once a malignant hub referred to as black hole goes into the framework. Black hole center point exhibits its fake lead among the methodology after all disclosure. Currently, varied strategies are made arrangements for Mobile ad-hoc networks. Regardless, at interims seeing Black hole or fake hubs, the entire Mobile ad-hoc frameworks are exposed to various sorts of assaults or network attacks. Among these issues, a black hole center points plugs itself of getting a nearest targeted hub, whose data packet must be constrained to drop. In this flooding procedures, if the communication from the genuine hub accomplishes later than the fake hub replies as requested by the standard hub. A false communication path is framed through a fake center hub. A perfect method is one in which the package reach to target with less delay and lesser overhead.

In this paper, this study talks about the implementation of Ant Colony Optimization Technique and Repetitive Route Configuration with Reactive Routing Protocol for obstruction of Black Hole Attack in Mobile ad-hoc networks. This study revealed the results with more valuable throughput and better prevention of Black Hole Attack by using ACO with Reactive Routing Protocol and achieved 10% of higher throughput and 27% of less Packet Loss over Least Cost Path Protocol.

KEYWORDS: Black Hole Attack; Ant Colony Optimization; Reactive Routing Protocol; Secured ad-hoc network.

1. Introduction

The Mobile ad-hoc networks (MANET) consists of the frameworks of transportable registered devices related remotely that are not encouraged of settled foundation [25]. There are small number of characteristics of MANET that are the following: 1) there is no might want of settled structure, 2) the architecture of the framework is versatile and dynamic, and 3) only two hubs are required for a wireless connection in a wireless medium. The wireless medium [4] is not secure as wire framework, the MANETs are auto handled portable frameworks of freely moveable hubs. It can work separately and can be connected to the settled framework. There will be some constraints as of data measure Constraints and Energy limitation, disseminated nature of activity for security, guiding and have course of action, a great deal of flexible than mounted Network, High customer thickness and escalated dimension of customer portability, Nodal network is intermittent and every center set about as each host and switch. On the contrary hand, their square measure has a few issues in Mobile ad-hoc networks that are: aimlessly consistently evolving topology, restricted energy, no incorporated administration, capacity and danger from compromised hub inside system.

MANET has some security standards that can guarantee wellbeing of system. These are: Accessibility, Reliability, Secrecy, Realness, Approval, Non-Reputation and Concealment [43]. There are two categories of attacks in MANET.

Passive Attacks: These types of attacks are not for steering convention rather than effort for catching fundamental data by means of movement's investigation. Due to this sort of attack, the secrecy of message is traded off. Uninvolved attacks incorporate Overhearing, Position revelation, and Traffic examination.

Active Attacks: Dynamic attacks, the interlopers adjust, infuse, manufacture, create or change information packets. This outcome in loss of uprightness of information bundle. Dynamic assault aggravates working of system and its very critical than remote attack. Active attacks can interchange the data or redirect the path of packets. If a hub wants to send data to target hub, it sends packet to its nearest hub and that will send data to next nearest hub. Thus, this cycle will run until the packet reached to its proper destination. The packet loss happens when any defected hub opposed to sending the information to its correct recipient. For saving the energy when a hub is not connected to other hub for packet travelling, it turns itself into sleep mode.

Different types of attacks are described as follow:

Sleep Deprivation: This type of attack interfaces through other hub in such method that gives off an impression of being true blue, yet the motivation behind the communication is to keep the casualty hub out of its energy preserving rest mode [30].

Black Hole Attack: This type of attack is very dangerous because it simulates the packets received to its correct destination and opposed forwarding of data packets to its destination [39]. It is also known as full packet dropping attack [13]. During route discovery the black hold node shows itself as a valid route towards destination or sometime show itself as a valid destination [14].

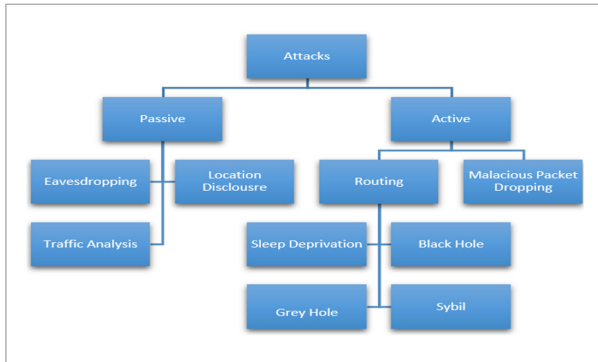
Gray Hole Attack: In the Gray Hole Attack, the malevolent hub drops a portion of the bundle or send parcel to wrong hub. Every hub of MANET needs an address through which hubs are recognized [30].

Sybil Attack: In this type of attack, the malicious hub makes the network path improper by diving the networks, this leads to shortage of resources for a network. It can also create the routing loop so that the

packet cannot receive to its correct destination [30]. Figure 1 illustrates the classification of network layer attacks in MANETs.

Figure 1

Classification of network layer attacks in MANETs [24]



Objectives and Motivation

The security and ensuring of accurate data communication between the origin and its destination in any network is the first priority. An attacker can use any hub, to make it malicious for spying the data and send it to attacker other than its destination path. The main objective of this research is to prevent the Black Hole Attack, increase the throughput and reduce the number of packet loss during finding the actual destination hub.

Normally, portable devices are not enriched with powerful resources and require an algorithm that use less resources for its implementation and create the ad-hoc networks.

As this study is focusing on prevention of Black Hole Attacks in MANET, the path finding and route optimization technique can be selected among these meta-heuristics simple, basic and advanced techniques of Ant Colony Optimization [9], Particle Swarm Optimization (PSO) [26], External Optimization [45, 46], Large Neighborhood Search [17] and Neuro-Heuristic Methods [31].

We chose Ant Colony Optimization (ACO) because the PSO has poor local optimization capability and premature convergence [8]. The Neuro Heuristic Methods needs massive amount of data for deep learning and utilizes large resources that is not available in portable devices with ad-hoc networks. ACO provides more classification accuracy than PSO with dataset having

large number of attributes [37] and utilizes very less resources [29]. It endorses that it utilizes the network coding resources in better way. It is now used in latest projects like path finding for unmanned vehicles [44] and Path Planning for Mobile Robots [9].

This study also used the Reactive Routing Protocol to reduce the packet loss and network load in mobile ad-hoc networks because this protocol ensures the packet delivery at destination with very low cost, less routing delay and minimal network load [13, 21].

The focus of the paper lands on Black Hole Attack and its prevention in MANET using Ant Colony Optimization (MAX-MIN Ant System (MMAS)) and Repetitive Route Configuration with Reactive Routing Protocol. Rest of the paper is organized as follows. Related work is reviewed in Section 2. Section 3 is about the proposed model; results are discussed in Section 4 and finally conclusion is drawn in Section 5.

2. Related Work

Black Hole Attack [39] is one of the genuine attacks in portable unarranged networks. In this type of attacks, a single node or more than one node becomes the malicious node and start dropping of packets instead of forwarding them to their correct position. [17, 28]. In this type of attack, a node simulate itself as the shortest path of network and collect all the data that were sent to original node. By sending the fake replies it can act as spy node and can create the denial of service attack [27]. Black Hole Attack can be distributed into two types of attacks (i) Single hub attack, in which a single node starts dropping the packet; (ii) Multiple hubs becomes the malicious nodes and starts to drop the data packets known as Gray Hole attack. The Black Hole Attack has two kind of properties that a node can simulate itself as the shortest path towards the target means showing the fake path. The malicious node can drop the packets as well.

The other name of Black Hole Attack is Sleep Deprivation attack that can be created through remotely outside the system. By attacking, the attacker can use any hub, to make it a malicious hub, this malicious hub can spy the data and send it to the attacker and stop sending the packets towards its destination path [2]. Numerous systems are proposed to stay away from and recognize the Black Hole Attack [27]. For

this, below some techniques are presented with their advantages and drawbacks.

In [25], multiple solutions are proposed to avoid attacks of Black Hole. In first, techniques (Detection by checking destination sequence number), it describes to find multiple paths of the destination but it creates too much issues, such as the time delay or higher latency. It can also create the bounces of data packets between the hubs. In other techniques, send packet bundle that have number of misuses packets in the bundle. The second technique, Detection, Prevention and Reactive AODV (DPRAODV) [16] is better approach for finding the malicious hub. but this technique utilized a large memory because there is need of two different tables, one for storing the last successful data sending address for every hub and second for counting the successfully transaction in packet sending and receiving for every hub. This paper only focusses on single hub attack in the system.

The specific procedure (Detection of black hole on AODV by Deng) [29] is considered to distinguish the Black Hole Attack with its interests and difficulties. Authors talk about two types of attacks, in which one is attack with single hub Black Hole and the other is attack with multiple Black Hole hubs. In this article, researchers TRIPO is a better way. It recognizes invading hub and as well as strengthens system centers to close different hub packages.

The Remote system [38] is proposed for the avoidance of Black Hole Attack. In this proposed system, there is no need of any extra equipment and changing in physical system. This system uses the Ad-hoc On Demand Multipath Distance Vector technology [19]. In this system, every neighboring hub keeps validity of its neighbor; that is why this protocol needs least extra time without anxiety hub and decrease bundle loss as portable enhancement.

Two Security methods processed under the process of executing, Integration Detection systems and Way-Sharing techniques [34]. The executable grid used to inspect is the access element and the accuracy factor. The result shows that availability of Watchdog and Path Rater (WPR) [34] is better than anything else than measuring availability. The paper considers different types of separate and dynamic attacks.

Consider how SMC [40] arrangements can be used to protect security. SMC is a short type of secure mul-

tiple accounting. After a while, physically distributed processing gadgets in a single system may want to reflect, some of the capabilities of their private partnerships, without exposing these partnerships. Comes under a securely protected multitask (SMC) class. SMC issues can be answered with information inputs or with some known methods in mobile-shared networks. The authors reviewed further security issues of MANETs as well.

Another barrier space frame that is arranged uniquely for MANETs, is called EAACK (Extended EAACK) [15]. The authors indicate additional interest to apply for application. Three weaknesses of the EAACK is clock drop scheme, i.e. false lieutenant, limited transmission power, and receiver's collision. In this paper, the authors finished both Digital Signature Algorithm (DSA) [15] and RSA [33] in the suggested EAACK for implementation in MANET. Public Delivery Ratio and Routing Over [15]. As a result, they show that EAACK is an important project that is equipped to isolate the wrong-troubleshooting report. The DSA depends on the RSA that is less than the least dependent on the RSA. DSA is a computerized signature in management. EAA started aggression by launching a custom attack.

A fuzzy logic-based component is proposed to identify the Black Hole Attack with an Ad Hoc On-Demand Distance Vector (AODV) convention [18]. Execution grounds used to control the transmission rate, enhance execution rate, and reduce network delay checking. Based on fuzzy logic, hangout increases device throughput. This component based on Fuzzy Logic can also be used similarly in the Gray Holes and Worm Holes attacks.

3. The Proposed Model (Black Hole Attack Prevention Using MAX-MIN Ant System)

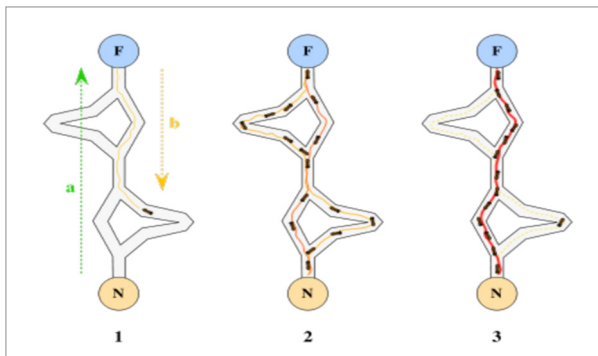
The Prevention of Black Hole Attack in Mobile Ad-Hoc Networks by implementing Ant Colony Optimization (MAX-MIN Ant System (MMAS) [3] and Repetitive Route Configuration with Reactive Routing Protocol is proposed. This technique has two main steps, the first one is Route Discovery and the second one is Route Maintenance. In the first step, Route Discovery,

Ant Colony Optimization (MAX-MIN ANT System) technique is used. After finding the Route Discovery, the Route Data is saved in Reactive Routing Protocol Formats [1, 4]. The Reactive Routing Protocol works on Demand as any device need to send data so the Route Configuration is done repetitively according to need of data sending among the nodes [35].

Adopting the Route Discovery using Ant Colony Optimization: The Ant Colony Optimization algorithm has been inspired by real-life [31], which is roaming around its homes for forces to investigate nutrition inquiry. Ants navigated from the nest to eat; they discovered the smallest way through the Pheromone. Ants run randomly; Pheromone is collected on every path. On the way as a maxim, the chances of following it increases. If we are trendy, in some other ways, the essential idea of metaphoric metabolism in the area of underground bugs is to take real chess foods. To find the shortest way, a non-static compound system known as pheromone is removed from underground insects. It is when insects are returning home after stopping food search and leaving the way. Pheromone Ants can also see Pheromone and there is a tendency to carry after high possibilities, which focuses on the methods described by Solid pheromone [6], known as a little bit of control bundle with a kind of personality, which is used to find their way towards the goal. Due to its strength and versatile nature, the Ant Colony Optimization (AOC) can find its applications in this steering, work and plan [20]. Similarly, it is used as part of biotechnology and communication systems. In Figure 2, the path shows use of Ant-colony Optimization techniques [41]. The path Segments are accumulated by the Virtual Trail on possible paths from starting node in Figure 2.

Figure 2

A Route-Finding using Ant Colony Optimization



As the amount of Trail present increases from the starting node, the path selection at random bases increases. It shows the direct proportion between the Trail presence and the Path Selection [7]. On Each Node, the Ant Selects the next path by the pheromone level. The ant continues to select the path with pheromone level until they reach the starting node. The Meta Heuristic Method is used in Ant Colony Optimization to analyze the optimality among multiple paths [42]. This Heuristic method to solve the very common class of computing issues by combining the Heuristic given to the user in the hope of getting an effective way. We choose soft computing technology to solve difficult computing.

Implementation of Meta-heuristic Technique in Ant Colony Optimization

The Following steps are used to implement Ant Colony Optimization [41].

Step 1: (Set Parameters [i, j, T, K, P, L, T_{min} , T_{max}])

Step 2: Implement Solutions of ACO.

- a The path will be followed with possibility from node i to j.

$$\text{The possibility of i and j} = \frac{(T_{i,j}^\alpha)(\eta_{i,j}^\beta)}{\sum (T_{i,j}^\alpha)(\eta_{i,j}^\beta)}. \quad (1)$$

Step 3: Increase amount of pheromone as per equation

$$T_{i,j} = T_{i,j} + (1-P)T_{i,j}^p \quad (2)$$

where L_k is the cost of the k_{th} ant's tour (typically length)

Step 4: Virtual trail accumulated on path segments

There are many cases of the ACO meta-heuristic among these, Ant System, Ant Colony System (ACS) and MAX-MIN Ant System (MMAS) are commonly used [42]. We opt the Max Min Ant System (MMAS) for this research paper.

Step 1: On Completion of tour the Pheromone will be updated by each ant.

Step 2:

$$T_{i,j} = (\sum_{k=1}^m (T_{i,j}^k)) + (T_{i,j})(1-P), \quad (3)$$

Pheromone disappearance quantity is P, K is number of travels from node i, to j for an ant in $\Delta T_{i,j}^k$ and m is total number of ants.

Step 3:

$$T_{i,j}^k = \begin{cases} 1/L_k \\ 0 \end{cases} \Delta \quad (4)$$

If 'K' ant travels from node i to j

The length of travel between node i, to j is L_k .

Step 4: the minimum and maximum pheromone quantity is limited by the m number of ants.

Step 5: The $T_{i,j}$ will never go outside the T_{\min} and T_{\max} .

Step 6: The $T_{i,j}$ will assigned to T_{\max} in case of i and j value greater than T_{\max} or $T_{i,j}$ will assigned to T_{\min} in case of $T_{i,j}$ value less than T_{\min} .

Route Maintenance Using Reactive Routing Protocol

Reactive Routing Protocol is also known as request steering protocol [25]. The reactive routing protocol is required for the transmission of information. The benefit of this protocol is that it reduces the route Discovery time during constant transmission of data bundles. Ad Hoc Demand Distance Vector (AODV) [12, 35] and Dynamic Source Routing (DSR) [29] is the instances of the reaction routing protocol. In AODV, each node records the next hub address in its routing table. It executes the route Discovery process when there is no address of destination hub in the source routing table. The source hub asks the next hub (to begin the search process of the RREQ) bundle. All hub receives RREQ bundled data on your steering table with a hub data, then sends a path to the source center (RREP). When the main source hub routing table is changed or dissolved, it starts the routing maintenance service. The source center is taught by a Reactive Root Error (RRE) bundle. DSR centers have to keep their way through the center. The DSR process reduces the system's data flow and evaluate the paths with a high time of data reachability [29].

As far as the ant columns optimization techniques are pulled out, the way the response can be saved in the Reactive Routing protocol [10] is as follows:

- a Table 1 shows the format to save the routing set of packet in Routing Protocol.
- b The format to maintain the data structure details maintained by each mobile node.

Packet Formats of Routing Packet's example Values used for Packet Formats of Routing Packets.

Table 1

Parameter with default values

Parameter Name	Values
Packet Type	Set to 1
HPC Hop Count	Set to 0
RCT Route Cost	Set to LCT Neighbor List
DIN (Dis Identification No)	Set to DIN_Table parallel to T
SVR Sender of VER Packet	Set to O (Originator node 'O' has packets to send to a Target node T)
ORG Originator Address	Set to O
TGT Target Address	Set to T
K Dis_Targets	Set to 1
DIV Dis_Via_Address	Set to O
DIT(1) DIS_Target_Address	Set to N
N Count of Neighbors Node	Set to Noda A of Neighbor List
DIT Dis_Target_Address	Set to A
NBR(1)(N)	Set to Neighbor List
LCT(1)(N) Link Cost	Set to Neighbor List parallel to NBR(1)(N)
RON Route Number	Allotted Route No by Router
NT Next Hop toward target	Set to A
NNO Next to Next Hop	ORG entry of Routing_Table
INT Invalid Type	Set to 1
SIN Sender of Invalid Packet	Set to A
RPO Repairing Originator Address	Set to A
RPT Repairing Target Address	Set to C

Note: 'O', 'T', 'N', 'C' and 'A' means IP Addresses of nodes 'O', 'T', 'N', 'C' and 'A'

Variables definition:

- HPC = Hop Count value
- RCT = Route Cost
- DIN = Dis Identification No
- ORG = Originator Address
- TGT = Target Address
- DIV = Dis_Via_Address

- N = Count of Neighbors Node
- NBR = 1st Node Value
- LCT = Link cost Value
- RON = Route Number
- NNO = Next to Next Hop
- SIN = Sender of Invalid Packet
- RPO = Repairing_Originator_Address
- RPT = Repairing_Target_Address

4. Results and Discussion

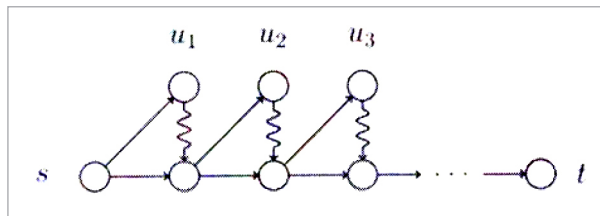
Theorem (λ -MMAS algorithm Theorem No 8. using directed graph with pheromone bounds) [3] is applied for testing.

Between two weight capabilities, Rapid continuous may be required in each vertex above 2Ω (n) ants so that $\sigma \leq 0.5 - \Omega$ (1) for the λ -MMAS as well as the possibilities of building the shortest path in each step of next iteration.

The hypothesis is demonstrated by illustration: this study demonstrates its performance in Figure 3, chart with the $k = \Omega$ (n) triangle, increase capabilities between W1 and W2 (W1 and W2 are the weight functions) during each repeat. It is necessary that λ -MMAS requires $\lambda = 2\Omega(k) = 2\Omega(N)$ units should be started in each vertical to maintain continuous possibilities for each of the lowest hostages. During every repetition, the λ -MMA is not a priority in this setting because the shortest methods for W1 and W2 are quite unique, and λ -MMAS cannot save unrecognized arrangements in pheromone remembrance.

Figure 3

From s to t path different equating triangles



λ -MMAS - Consider the Reproduction of the Performing State of the MMA. Ideally, let sort the triangle as ideal weight work if the pheromone

estimates are not less than 0.5 on the shortest possible route. On the occasion that the $k/2$ triangle is positive, the need for the various ants that require a variety of kits, because at any rate, anybody at any rate is capable of any active circular segment at any rate. There is no need to settle on the decision. Event $k/2$ weak triangle Give chance to PS to make one of the units a right path, the possibilities of PP are that a specific anti-accurately examines $k/2$ negative triangle, and $P1 \leq 0.5$ be is likely to Antioxidants effectively find a particular trouble triangle on this point

$$p_s \leq 1 - (1 - pk)^\lambda \leq 1 - (1 - (0.5)^{k/2})^\lambda \leq \lambda \cdot 2^{-k/2}. \quad (5)$$

For ensuring that PS is not less than continuous, at least $2\Omega(c)$ units can begin.

On the occasion that triggers are very good in the present repetition, a number of tricks $\tau \geq 0.5$ will need to develop the shortest path. One of the most recent ways to achieve the precession is to reduces down the values in a triangle with minimum angles. At this time the same triangle respects the perimeter on the other circular segment. In the following recurrence, this curve will be the shortest way, and its perimeter will be the maximum $0.5 + \sigma$. For a length of 0.5σ , the $PS \leq 0.5 + \sigma$ number of units can begin with the initial number.

Thus, for the λ -MMA, the minimum triangle quantity is not needed at least the repetition.

The ability to perform a close exam may be in a desire to work for some special work near some permanent division of the triangle. This means that every repetition requires a number of exponential ants (to be opposed to the minimum continuous disposition in this premium authentication) for the limited extent to the right extent in the optional recurrence guarantees the minimum chances of malicious nodes.

As a rule, [22], the reduction rate, the low impact effect is on the pheromone fields, reducing the predictions of the W1 predictions of the start of refining method that ants will start moving more than T, and it will reduce the W1-favored circular segment. Arbitration will have to be faced, due to fluctuations, the concerns presented by the introduction of the procedure will reduce the path between s and t. In this event that the number of triangles supports W2 to W1, by w1 side w2 side w1-favoring triangles W2 by W1 amid

W1. The fortress will be fortified by the W1 during the maintenance.

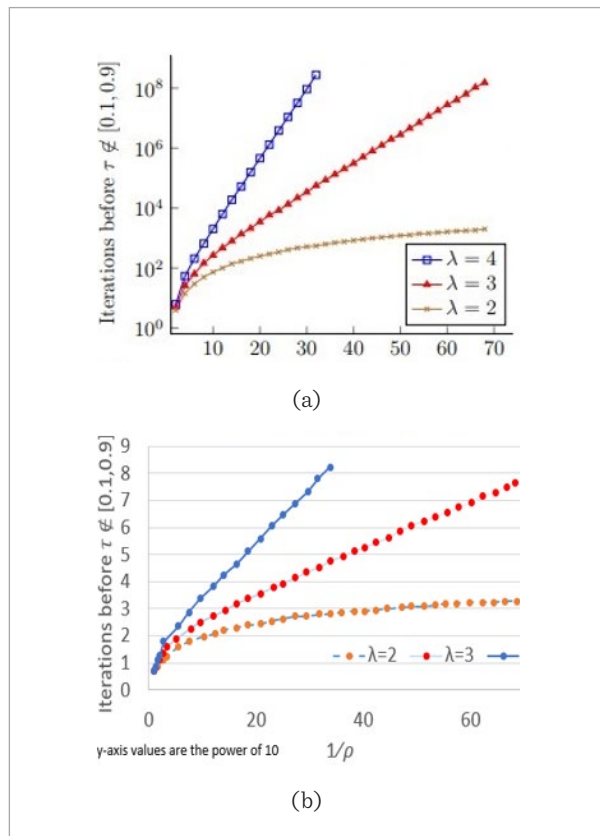
Nevertheless, the case described the problem of route stability, pheromone memory is not suitable for isolating two weight capabilities, and then it is not well-scale if the differences between weight capabilities reach different vertical lines.

Implementing the Experiment

The settings presented in previous results were carried out outside different re-operations to determine the λ -MMAS functionality; in this section all the middle points and modes introduced in the data are MMAS parameters σ and λ , and the proper continuous flow of time, where information is available from every suitable 1000 compounds.

Figure 4

The number of arbitrarily pheromone before leaving the triangle blue [0.1, 0.9] triangle to remove the rate of triangle before the procession λ - MMA started with the same repeat on each with $\lambda = 2, 3, 4$ vertices [22]

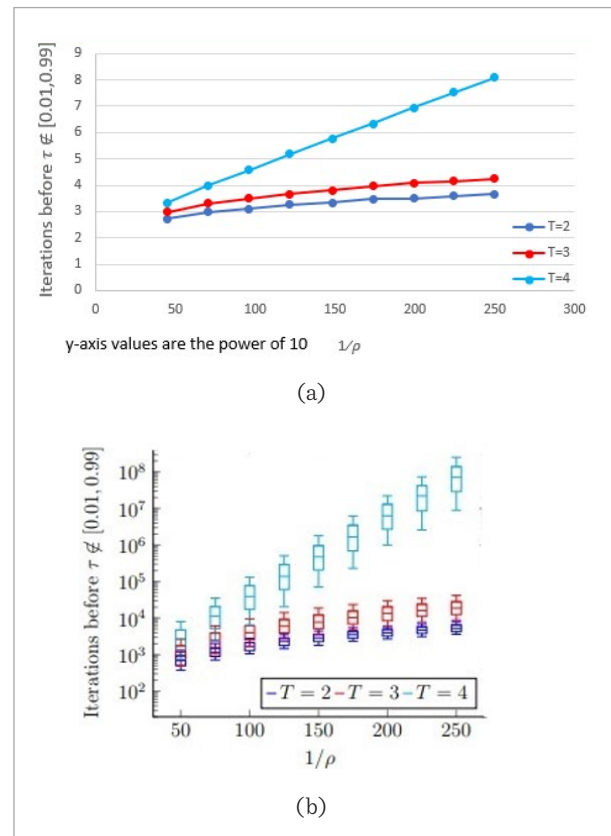


To change the path order with the balance of λ -MMA 2 began with each vertical 2 less then equal to λ greater then equal to 4 ants, resumed with different expansion rates, the principal range recording, which contains estimates on the pheromone triangle [1/10, 9/10] left range (e.g. blue out) that appear in Figure 4, with $\lambda = 2$, $\lambda = 3$ and $\lambda = 4$.

The curve is practiced, which suggests that the $\lambda = 2$ units are not enough to maintain pyramidation due to its compilation super-polymerum numbers, it appears that enough to meet $\lambda = 3$ units. For 1 MMA in close proximity, an anti-province has been re-activated with the extent of the expansion rate and the length of the phase, recording a significant repeat on which the Peruvian triangle specific boundaries remain on the triggers circular segments. The result in Figure 5, all of its goals are a significant difference between $T = 2$, $T = 3$ and $T = 4$. In addition, it appears that the Pheromone Field should be in such a way to stay

Figure 5

The native variations with slow impulsions tours



in excess of $[0.01, 0.99]$ to prohibit it. λ -MMA was re-replaced with $\lambda = 6$ and $\sigma = 1/50$ in the world's changes in order with $K = 200$ triangle. The number of triangles was recorded outside $[1/4, 3/4]$.

The Pheromone Field; Figure 6, shows the slightest number of triangles with the pheromones estimates outside the circle. By increasing the weight of the triangle increases the increasing number of weights, and in the end solution, for example, in the $[1/4, 3/4]$ pheromone area, approximately 33% covers the triangle area. Figure 6, triangle arrangements is more important than the number of W1 triangles associated with the W2 triangle. The curve is practiced, which suggests that the units are not enough to maintain pheromone due to its compilation super-polymerous numbers, it appears that it is enough to meet units between $T = 2$ and $T = 3$.

In Figure 7, similarly mathematics in the setting of changes in the world with the rate of disappearing in $\sigma = 1$ to increase the effect of repetition. As a result of some extent, even with this unusual error rate,

Figure 6

200 triangles in arrangement; normal crosswise over 1000 reproductions; where λ equal to 6 and p is equal to 1/50s

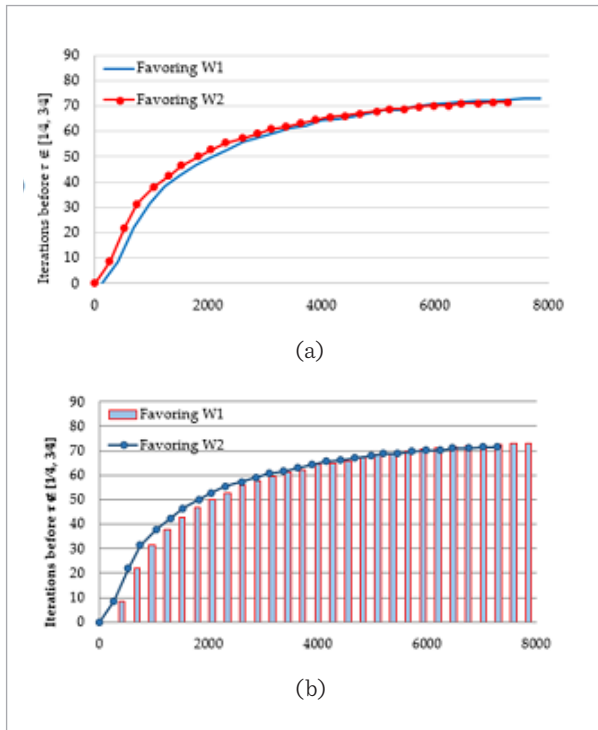
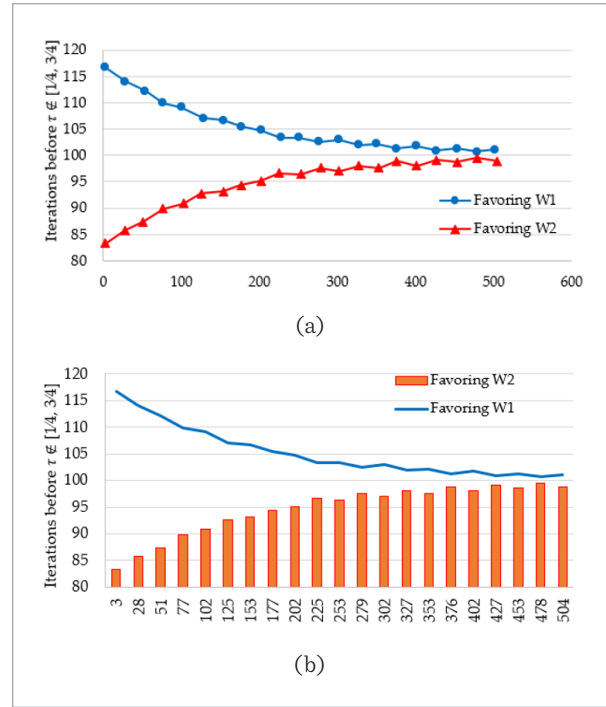


Figure 7

Across more than 1000 radio drives, 200 triangles in sequence; $\lambda = 6, \rho = 1$



the proportion between the weight triangles ratio is strong between the W1 and W2 to support W2 ratio which is just 3:2. After some time, it appears that the effect of basic prediction is balanced, as opposed to maximum. In addition, it appears that the information focuses interchange between iterations utilizing W1 and W2, making the lines seem spiked.

5. Limitation of Proposed Work

As study is focusing on prevention of Black Hole Attack in MANET by implementing the Ant Colony Optimization with Reactive Routing Protocol, following are the limitations of our work.

- 1 It is not efficient for large-scale network
- 2 The limitation of this study is to eliminate the malicious hub for its first time.
- 3 The convergence time has uncertainty and depends on selection of pheromone related parameters.

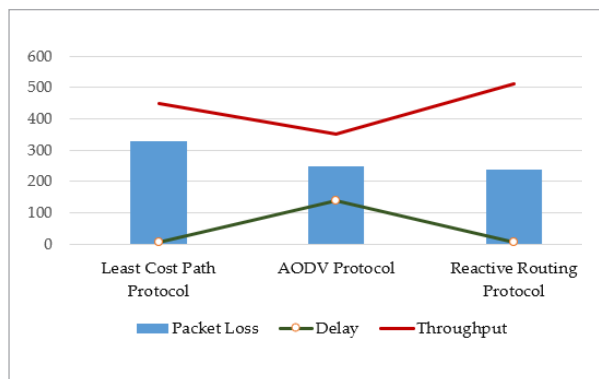
6. Comparison of Results

In April 2019, a research work for Preventing the Blackhole attack with implementation of Ant Colony Optimization was presented by two authors Kaveri Sawant and Dattatray Sawant [31]. In that research the authors achieved the 449 throughputs and 328 packets loss with 10 number of nodes by using Least Cost Path Protocol. In simple AODV protocol, they achieved the 350 throughput and 250 packets loss with 10 number of nodes.

In our model, the better results are achieved with 513 throughputs and 237 packets loss with 10 number of nodes by using Reactive Routing Protocol. Comparison is shown in Fig 8.

Figure 8

Comparison chart of throughput and packet loss by using ant colony optimization with reactive routing protocol and other protocols with 10 number of nodes



Therefore, we conclude that Ant Colony Optimization with Reactive Routing Protocol gives better throughput and provide better prevention of Black Hole Attack with minimum number of chances of occurrence than existing approaches.

References

1. Aastha, M., Shweta, S. Comparison of Manet Routing Protocols. *JCSMC*, 2019, 8(2), 67-74.
2. Al Dulaimi, L. A. K., Ahmad, R. B., Yaakob, N., Yusoff, M. H. M., Elshaikh, M. Black Hole Attack Behavioral Analysis General Network Scalability. *Indonesian Journal of Electrical Engineering and Computer Science*, 2019, 13(2), 677-682. <https://doi.org/10.11591/ijeecs.v13.i2.pp677-682>
3. Aleem, A. Evolution of Ant Colony Optimization Algorithm - A Brief Literature Review, 2019, arXiv:1908.08007v2 [cs.NE]
4. Alfa, A. A., Sadiku, A. A., Misra, S., Adewumi, A., Ahuja, R., Damasevicius, R., Maskeliunas, R. *An Effective Wireless Media Access Controls Architecture for Content Delivery Networks*. Springer International Publishing, 2018, 942.

7. Conclusion

Mobile Ad-hoc Network compromises with major issue known as Black Hole Attack. A wide range of researchers proposed different procedures for the anticipation of malicious node attack. In this research, Ant Colony Optimization Algorithm λ -MMAS is used to deal with accurate route discovery in mobile ad-hoc networks. Expanding past results about single MMA's unusual example, focusing on a vertical ideal process using every type of ideal state λ node. We have shown that the λ -MMAS can also manage the most dynamic paths in a constant number of times per unit. Comprehensive compare arrangements (by maintaining the proximity of approximately 0.5 premiums for its effects). Changes in brain-boggling tasks can be checked in the λ -MMAS settings. For example, with the constant phase length, reducing the results of the malicious routes, consisting of two weight capabilities, and malicious route reduction. After finding the Route Discovery the Route Data will be saved in Reactive Routing Protocol Formats. The Reactive Routing Protocol works on Demand as any device needs to send data so the Route Configuration will be done repetitively according to need of data sending among the nodes. As we use reactive routing protocols, this will eliminate the above-the-resolution solution, because of their ant colony optimization (MAX-MIN anti-system), which has low-end head issues and reactive routing approach will be guided to prevent data loss during transfers and also prevents Black Hole Attacks. This study also presented the comparison of throughput with different protocols and presented the results that Least Cost Path Protocol has gave less throughput of 449 and 328 Packet loss with 10 number of nodes. The Ant Colony Optimization with Reactive Routing Protocols gives maximum throughput of 513 and 237 packet loss with 10 number of nodes that our study provides more valuable throughput and better prevention of Black Hole Attack.

5. Alfa A.A., Misra S., Adewumi A., Salami F.O., Maskeliūnas R., Damaševičius R. (2018) Implementation of MANETs Routing Protocols in WLANs Environment: Issues and Prospects. In: Antipova T., Rocha Á. (Eds.) *Information Technology Science. MOSITS 2017. Advances in Intelligent Systems and Computing*, 724. Springer, Cham. https://doi.org/10.1007/978-3-319-74980-8_24
6. Anchugam, C. V., Thangadurai, K. Detection of Black Hole Attack in Mobile Ad-hoc Networks Using Ant Colony Optimization - Simulation Analysis. *Indian Journal of Science and Technology*, 2015, 8(13). <https://doi.org/10.17485/ijst/2015/v8i13/58200>
7. Caihong, M., Jian, Z., Multi-Objective Ant Colony Optimization Algorithm Based on Decomposition for Community Detection in Complex Networks. *Soft Computing*, 2019. <https://doi.org/10.1007/s00500-019-03820-y>
8. Chen, G., Liu, J. Mobile Robot Path Planning Using Ant Colony Algorithm and Improved Potential Field Method. *Computational Intelligence and Neuroscience*, 2019. <https://doi.org/10.1155/2019/1932812>
9. Dai, X., Long, S., Zhang, Z., Gong, D. Mobile Robot Path Planning Based on Ant Colony Algorithm with a* Heuristic Method. *Frontiers in Neurorobotics*, 2019, 13(15). <https://doi.org/10.3389/fnbot.2019.00015>
10. Darabkh, K. A., Judeh, M. S. E. An Improved Reactive Routing Protocol over Mobile Ad-hoc Networks. 14th International Wireless Communication Mobile Computer Conference. (IWCMC), 2018, 707-711. <https://doi.org/10.1109/IWCMC.2018.8450367>
11. Eskandarpour, M., Dejax, P., Péton, O. A Large Neighborhood Search Heuristic for Supply Chain Network Design. *Computers & Operations Research*, 2014, 80. <https://doi.org/10.1016/j.cor.2016.11.012>
12. Gupta, P., Goel, P., Varshney, P., Tyagi, N. Reliability Factor Based AODV Protocol: Prevention of Black Hole Attack in MANET. *Proceedings of ICSICCS-2018*. https://doi.org/10.1007/978-981-13-2414-7_26
13. Guru, C., Chauhan, S. A Dynamic Threshold Based Algorithm for Improving Security and Performance of AODV Under Black-Hole Attack in MANET. *Wireless Networks*, 2017, 1-11. <https://doi.org/10.1007/s11276-017-1622-y>
14. Guru, C., Chauhan, S. Performance Analysis of Black-Hole Attack Mitigation Protocols Under Gray-Hole Attacks in MANET. *Wireless Networks*, 2017. <https://doi.org/10.1007/s11276-017-1639-2>
15. Hmouda, E., Li, W. Detection and Prevention of Attacks in MANETs by Improving the EAACK Protocol. *Conference Proceedings of IEEE SOUTHEASTCON*, 2018, 1-7. <https://doi.org/10.1109/SECON.2018.8478999>
16. Imad, I. S., Majdi, Z. R. Various Solutions of Black Hole Attack in A mobile Ad Hoc Network (MANET). *International Journal of Computer Science and Information Security*, 2018, 12(8).
17. Kaur, H. The Approach for the Prevention of Black Hole Attack in MANET using DSR Protocol and Ant Colony Optimization Technique: A Review. *IITM Journal of Management and IT*, 2016.
18. Kumar A.K., Rana, J. L., Jain, R. C. Detection of Wormhole, Blackhole and DDOS Attack in MANET Using Trust Estimation under Fuzzy Logic Methodology. *International Journal of Computer Network and Information Security*, 2017, 9(7), 29-35. <https://doi.org/10.5815/ijcnis.2017.07.04>
19. Kumar, V. R. Secure Adhoc On-Demand Multipath Distance Vector Routing in MANET. *Proceedings of the International Conference on Computing and Communication Systems*, 2018, 49-63. https://doi.org/10.1007/978-981-10-6890-4_5
20. Kuo, R. J., Zulvia, F. E. Hybrid Genetic Ant Colony Optimization Algorithm for Capacitated Vehicle Routing Problem with Fuzzy Demand - A Case Study on Garbage Collection System. *The 4th International Conference on Industrial Engineering and Applications (ICIEA)*, 2017, 244-248. <https://doi.org/10.1109/IEA.2017.7939215>
21. Lanjewar, A., Gupta, N. Optimizing Cost, Delay, Packet Loss and Network Load in AODV Routing Protocol. *International Journal of Computer Science and Information Security*, 2013, 11(4), arXiv preprint arXiv:1304.6486
22. Lissovoi, A., Witt, C. Runtime Analysis of Ant Colony Optimization on Dynamic Shortest Path Problems. *Theory of Computer Science*, 2015, 561, 73-85. <https://doi.org/10.1016/j.tcs.2014.06.035>
23. Majumder, S., Debika, B. Comparative Study Between Modified DSR and AODV Routing Algorithms to Improve the PDF Due to Wormhole Attack in MANET. *International Journal of Scientific Research and Review*, 2019, 8(1), 1095-1102.
24. Meddeb, R., Triki, B., Jemili, F., & Korbaa, O. A Survey of Attacks in Mobile Ad Hoc Networks. *Proceedings of International Conference on Engineering and MIS (ICEMIS)*, 2017, 1-7. <https://doi.org/10.1109/ICE-MIS.2017.8273007>
25. Mishra, D., Arukonda, S. Black Hole Attack Prevention Techniques in MANET: A Review. *International Journal of Engineering and Computer Science*, 2014, 3(6), 6735-6738. ISSN:2319-7242
26. Mohamed, M. A., Diab, A. A. Z., Rezk, H. Partial Shading Mitigation of PV Systems via Different Meta-Heuristic

- Techniques. *Renewable Energy*, 2018, 130, 1159-1175. <https://doi.org/10.1016/j.renene.2018.08.077>
27. Mohammad, S., Singh, P., Dey, A., Jalal, A. S. ESMB-CRT: Enhance Security to MANETs Against Black Hole Attack Using MCR Technique. *Lecture Notes in Networks and Systems*, Springer, 2017, 319-326. https://doi.org/10.1007/978-981-10-8204-7_32
 28. Mohammed, A. S. Detection and Removal of Black Hole Attack in Mobile Ad Hoc Networks Using Grp Protocol. *International Journal of Advance Research in Computer Science*, 2018, 9(6), 1-6. <https://doi.org/10.26483/ijarcs.v9i6.6335>
 29. Ning, J., Zhang, C., Sun, P., Feng, Y. Comparative Study of Ant Colony Algorithms for Multi-Objective Optimization. *Information*, 10(1), 11, 1-19. <https://doi.org/10.3390/info10010011>
 30. Niranjana, P., Binod, K. P. Defense Against Co-operative Black-Hole Attack and Gray-Hole Attack in MANET. *International Journal of Engineering & Technology*, 2018, 7(3.4), 84-89. <https://doi.org/10.14419/ijet.v7i3.4.16752>
 31. Połap, D., Wozniak, M. Voice Recognition by Neuro-Heuristic Method. *Tsinghua Science and Technology*, 2019, 24, 9-17. <https://doi.org/10.26599/TST.2018.9010066>
 32. Ramalingam, S., Sujatha, P. An Extensive Work on Stock Price Prediction Using Ant Colony Optimization Algorithm (ACO-SPP). *International Journal of Intelligent Engineering and Systems*, 2018, 11, 85-94. <https://doi.org/10.22266/ijies2018.1231.09>
 33. Rasha, S., Abdeldaym, H. M. A. E. Modified RSA Algorithm Using Two Public Key and Chinese Remainder Theorem. *International Journal of Electronics and Information Engineering*, 2018, 10(1), 51-64.
 34. Rosas, E. Survey on Simulation for Mobile Ad-Hoc Communication for Disaster Scenarios. *Journal of Computer Science and Technology*, 2016, 31(2), 326-349. <https://doi.org/10.1007/s11390-016-1630-x>
 35. Sasidharan, D., Jacob, L. A Framework for the IPv6 Based Implementation of a Reactive Routing Protocol in ns-3: Case Study Using LOADng. *Simulation Modelling Practice and Theory*, 2017, 82, 32-54. <https://doi.org/10.1016/j.simpat.2017.12.007>
 36. Sawant, K., Sawant, D. Improved Network Lifetime and Secured Routing Against Blackhole Attack in Wireless Sensor Networks Using SRR. *IOSR Journals*, 2019, 14(2), 30-36.
 37. Selvarajan, D., Jabar, A. S. A., Ahmed, I. Comparative Analysis of PSO and ACO based Feature Selection Techniques for Medical Data Preservation. *International Arab Journal of Information Technology*, 2019, 16(4), 731-736.
 38. Singh, S., Mishra, A., Singh, U. Detecting and Avoiding of Collaborative Black Hole Attack on MANET Using Trusted AODV Routing Algorithm. *Symposium on Colossal Data Analysis and Networking (CDAN)*, 2016, 87, 5-10. <https://doi.org/10.1109/CDAN.2016.7570906>
 39. Tino, R., Merlin, R. R. Novel Trust Based Energy Aware Routing Mechanism for Mitigation of Black Hole Attacks in MANET. *Wireless Personal Communications*, 2019. <https://doi.org/10.1007/s11277-019-06120-8>
 40. Ul-Islam, B. K., Olanrewaju, R. F., Anwar, F., Najeeb, A. R., Yaacob, M. A Survey on MANETs: Architecture, Evolution, Applications, Security Issues and Solutions. *Indonesian Journal of Electrical Engineering and Computer Science*, 2018, 12(2), 832-842. <https://doi.org/10.11591/ijeecs.v12.i2.pp832-842>
 41. Wang, J., Cao, J., Sherratt, R. S., Park, J. H. An Improved Ant Colony Optimization-Based Approach with Mobile Sink for Wireless Sensor Networks. *Journal of Supercomputing*, 2018, 74(12), 6633-6645. <https://doi.org/10.1007/s11227-017-2115-6>
 42. Xu, H., Pu, P., Duan, F. Dynamic Vehicle Routing Problems with Enhanced Ant Colony Optimization. *Discrete Dynamics in Nature and Society*, 2018, 1-13. <https://doi.org/10.1155/2018/1295485>
 43. Yadav, N., Chug, U. Topologies, A. D. N., Secure Routing in MANET: A Review. *International Conference on Machine Learning, Big Data, Cloud and Parallel Computing*, 2019, 375-379. <https://doi.org/10.1109/COMIT-Con.2019.8862238>
 44. Yue, L., Chen, H. Unmanned Vehicle Path Planning Using a Novel Ant Colony Algorithm. *EURASIP Journal on Wireless Communication and Networking*, 2019, 2019(1). <https://doi.org/10.1186/s13638-019-1474-5>
 45. Zeng, G. Q., Xie, X. Q., Chen, M. R., Weng, J. Adaptive Population Extremal Optimization-based PID Neural Network for Multivariable Nonlinear Control Systems. *Swarm and Evolutionary Computation*, 2019, 44, 320-334. <https://doi.org/10.1016/j.swevo.2018.04.008>
 46. Zeng, G., Liu, H., Wu, D., A Real-Coded Extremal Optimization Method with Multi-Non-Uniform Mutation for the Design of Fractional Order PID Controllers. *Information Technology and Control*, 2016, 45(4), 358-375. <https://doi.org/10.5755/j01.itc.45.4.13310>

