# PGO-DLLA: Parallel Grid Optimization by the Daddy Long-Legs Algorithm for Preventing Black Hole Attacks in MANETs

Khalil I. Ghathwan
School of Computing, Universiti Utara Malaysia, Kedah, Malaysia;
Department of Computer Sciences, University of Technology, Baghdad, Iraq
Email: k.i.ghathwan@gmail.com, s93453@student.uum.edu.my

Abdul Razak Yaakub
School of Computing, Universiti Utara Malaysia, Kedah, Malaysia
Email: ary321@uum.edu.my

**Keywords:** mobile ad hoc networks (MANETs), black hole attack, swarm intelligence, malicious node, secure routing, optimization

**Received:** December 10, 2014

*Mobile ad hoc networks (MANETs) are wireless networks that are considered a good alternative to the other types of networks during the hardest times such as wars or natural environment disasters. MANETs have the capability of working without any need for base stations or infrastructures. However, MANETs are subject to severe attacks, such as the black hole attack. Many researchers in the field of secure routing and network security have been working on acceptable solutions to prevent black hole attacks in MANETs. Unfortunately, most of the proposals are not attainable or have performance difficulties. One of the most ambitious goals in the research is to find a way to prevent black hole attacks without decreasing network throughput or increasing routing overhead. Swarm intelligence is a research area for information models that studies the collective behavior of insects or animal swarms. Some algorithms have been proposed to address black hole attacks through new protocols and improving routing security with swarm intelligence. In this paper, we propose a parallel grid algorithm for MANETs that optimizes both routing discovery and security in an Ad Hoc On-Demand Distance Vector (AODV). The new technique, called Parallel Grid Optimization by the Daddy Long-Legs Algorithm (PGO-DLLA), simulates the behavior of the biological spiders known as daddy long-legs spiders. Experiments were conducted on an NS2 simulator to demonstrate the efficiency and robustness of the proposed algorithm. The results indicate better performance than the AntNet algorithm with respect to all metrics except throughput, for which AntNet is the better algorithm. In addition, the results show that PGO-DLLA outperforms the standard AODV algorithm in simulations of both a peaceful environment and a hostile environment represented by a black hole.*

*Povzetek: Razvit je algoritem za obrambo pred napadi na omrežja MANET.*

## 1 Introduction

Worldwide, there are more than 30,000 kinds of spiders, which are characterized by a unique way of hunting prey. Most types of spiders respond to vibrations that come from their web. Spiders have special methods for quick access to prey and capture them as soon as possible. Some vibrations coming from the web may signal a source of danger, and changing strategies is essential for avoiding the threat [1]. In this paper, we propose a new algorithm for parallel grid optimization that simulates the behavior of daddy long-legs spiders (PGO-DLLA). This type of spider responds to the first vibration that comes from the web and chooses the shortest path to catch the prey without giving it a chance to escape from the trap [2]. Spiders have a huge number of strategies to capture prey, such as trapping the prey in a sticky web [1], [2]. In the case of daddy long-legs spiders, all paths in the web are available for access to a destination, because daddy long-legs spiders do not use the glue that other spiders use. The absence of glue on the yarns of daddy long-legs spiders provides them with unique features, such as the ability to change their location in the web to avoid any dangers coming from outside the web. In addition, when there is more than one source of vibrations, the daddy long-legs spider chooses the smallest vibration frequency value to avoid the risk. This spider is sometimes called a hopper spider because it generates inverse artificial vibrations [2], which can be useful to tighten restrictions on its prey or to discard the prey when it is an unwanted kind. Daddy long-legs spiders are slightly different from other spiders because they have high sensing precision

using their eight legs, which act like sensors or agents to receive signals or to discover their prey's position.

A MANET contains many varieties of dynamic nodes. The network can be active in an actual environment without any infrastructure [3]. MANETs have numerous implementations in several fields, including emergency operations, military operations, civilian environments, and personal area networking [4]. However, they suffer from several limitations, such as short battery lives, limited capacities, and vulnerability to malicious behaviors. A black hole is one type of attack that occurs in MANETs. Black hole nodes attack routing protocols such as the AODV protocol [5], causing network packets to be dropped. The main goal of the AODV protocol is to find a path from a source to its destination node and then to forward the packets. The routing mechanism in AODV uses route requests (RREQs; for discovering routes) and route replies (RREPs; for receiving paths). However, this mechanism is vulnerable to attacks by malicious black hole nodes that can easily adjust the values of routing table fields such as *hop count* and *DSN* in order to deceive the source node after sending a RREQ, a source node will respond to the first RREP it receives. This RREP may be from a black hole node, and the source will not reply to other intermediate nodes. This could cause the end of cooperative work in MANET [3], [6], [7], [8], [9], [10].

Intensive computations are required to make AODV secure against black hole attacks [11]. Most of the proposed solutions with limited computations such as trusting neighboring nodes, using cross-layer cooperation, or allowing route redundancy are fail to detect cooperative black hole attacks [6], [8], [9]. However, use of intensive computations as a solution to cooperative black hole attacks may lead to depletion of the limited energy of batteries. In this paper, we develop methods to find the shortest secure path and reduce overhead using the information that is available in the routing tables [12], [13]. However, we use this information as input to propose a more complex algorithm using swarm intelligence. Mathematical formulas such as Hooke's law [14] and, Newton's second and third laws [15] are utilized to evaluate the route reply and choose the best path. For example, the vibration between two nodes, depending on Hooke's law.

The remainder of this paper is organized as follows Section 2 discusses some related work, Section 3 presents the proposed approach and methodology, and Section 4 presents the solution scenarios and parameters. Finally, Section 5 concludes the paper.

# 2 Related work

In [16], the authors proposed a new taxonomy to classify approaches to detecting black hole attacks in MANETs. This taxonomy classifies processes according to their computation: whether they are computationally limited or computationally intensive. In this taxonomy, the computationally limited approaches are simple processes that use network parameters, while the computationally intensive approaches use artificial intelligence techniques such as mobile agents, genetic algorithms, clustering, and fuzzy logic to implement the detection. Some approaches to detecting and defending against black hole attacks in MANETs are proposed in [6], [7], [8], [9], [10].

In [6], an anti-cooperative solution to black hole attacks that modified the standard AODV protocol was proposed. In the modified protocol, a source node does not respond directly when it receives the first RREP, but rather waits for a specific period of time. The source node has a cache list to save all RREPs and all details about the next hop that it gathers from other nodes. It then chooses the correct path from a list of response paths after checking for a repeated next hop node, and if there are none, it chooses a random path. The new contribution of this study was the use of a "fidelity table" and assigning fidelity levels to the participating nodes. The important point in their study is that it proposes a solution for collective black hole attacks. However, this method suffers from an increase in the control overhead, because of the exchanges of fidelity packets to achieve security.

In [7], a dynamic anomaly training method, which is one of the learning methods in data mining, was used. The authors create a database that contains the features that result from attacks to compare these with a regular network status. They use statistical theory to produce an anomaly threshold by measuring a projection distance. This method can detect black holes in AODV with low overhead, but false positives are a major drawback.

In [8], the authors suggested a method based on the fact that attackers rely on changing the destination sequence number to the maximum number and will therefore acquire the routing and drop the packets.

In [9], the authors suggested a computationally limited method to detect black hole attacks during the routing discovery in the AODV protocol. This method combines the technique of trusting neighboring nodes with a route redundancy message parameter. When intermediate nodes receive a RREQ from a source node, they send back a new RREP contain a sequence number (SN) to the source node. At the same time, the intermediate node will generate a newly defined SN request (SREQ) and send it to the destination node through the route. The destination node receives the SREQ message and sends a SN reply (SREP) message containing its SN. The source node saves each new SN that it obtains from the destination node in a special field of a SN table (SNT), for comparison with the current sequence source number. The exchanges of the RREQs, RREPs, SREQs, and SREPs in the entire network between the source and destination nodes increase the control overhead. This method is probably not effective in a large topology that has high mobility.

In [10], an algorithm was proposed that provides a security mechanism in AODV by trusting neighboring nodes based on feedback from other nodes and their reputations in the network. This is a distributed collaborative approach for ad hoc wireless networks. In this algorithm, each node does intrusion detection system (IDS) work locally and independently, but nearby nodes work together to monitor a larger area. Each node is

responsible for overseeing the activities involving local data. If an anomaly is detected in the local data, or if the evidence is not sufficient and requires a more comprehensive search, neighboring IDS agents cooperate on the global intrusion detection. However, this algorithm has a high routing control overhead.

# 3 Proposed approach and methodology

In this paper, we propose a new mechanism that works as an intelligent swarm algorithm based on the VDLLA algorithm, which is integrated into the AODV routing protocol. The new technique, which is intended to enhance security in the AODV protocol, is called Parallel Grid Optimization by the Daddy Long-Legs Algorithm (PGO-DLLA). It tries to reduce financial and technical constraints by reducing the number of hops in the route discovery for finding the destination. This algorithm is proposed in order to reduce the severity of black hole attacks and eliminate them.

## 3.1 Virtual Daddy Long-Legs Algorithm (VDLLA)

The VDLLA is a swarm of spiders. We assume that each spider has nine positions represented as a 3×3 matrix in a grid space, where eight of the positions are for the spider's eight legs and the center position is for the spider's body. Each spider evaluates the nine positions based on the objective function and determines the best location from the nine positions. The best position for each spider is then evaluated to choose a global position. The computational procedure of the VDLLA is as follows.

Step 1: Generate Initial population of spider members, considering N as the total number of members.

Step 2: Generate Initial location for each body of spider members randomly, and then calculate the legs position based on body position:
Assume the body position = (X, Y), the legs position is eight direction where: from up = (X,Y+0.1), from down =(X,Y-0.1), from left =(X-0.1,Y), from right = (X+0.1,Y), from up left = (X-0.1, Y+0.1), up right =(X+0.1,Y+0.1), from down left =(X-0.1,Y-0.1) and downright =(X+0.1, Y-0.1) as shown in Table 1 below.

Table 1: The positions of each agent (spider).

| | | |
|---|---|---|
| Leg5 = (X-0.1, Y+0.1) | Leg1 = (X,Y+0.1) | Leg6 = (X+0.1,Y+0.1) |
| Leg3 = (X-0.1,Y) | body = (X,Y) | Leg4 = (X+0.1,Y) |
| Leg7 = (X-0.1,Y-0.1) | Leg2 = (X,Y-0.1) | Leg8 = (X+0.1, Y-0.1) |

Step 3: Evaluate the fitness for each agent (spider) where the evaluation includes all position of agent (body + legs).

Step 4: Select the best fitness for each agent (spider) and save the position as best position.

Step 5: Select the global fitness from all best fitness and save the position as global position.

Step 6: Do while global fitness greater than tolerance value (tolerance value is based on objective function).

Step 7: Find new position for each agent where the body move to best position and legs position change based on body.

Step 8: Find new best fitness and new global fitness.

Step 9: If new global fitness less than global fitness.

Step 10: Global fitness = new global fitness.

Step 11: Else if new global equal global fitness

Step 12: Change the global position using (1) below:

$$Gpos_{new} = Gpos_{old} + 0.01(RND(1,d)) \quad (1)$$

Where, d is the dimension of objective function.

Step 13: iteration=iteration +1

Step 14: End while.

## 3.2 Problem formulation and solution representation

Aggregative conduct or swarm behavior in animals or insects is intelligent behavior of their biological group. The study of swarm intelligence is aimed at understanding the behavior of a group in nature. Biological scientists have found that many models can mimic the living systems of animals or insects.

Most spiders do not live in communities, so swarm intelligence does not reflect the collective behavior directly: rather, in this research we consider the sensitive behavior of spider legs to represent the collective performance. This approach is a relatively new orientation in the area of swarm intelligence. It is very important to develop new frameworks, which may be very useful in highly dynamic routing networks, in this area. We apply the new algorithm to MANETs, to address the problem of black hole attacks in the AODV routing protocol. The new proposal is based on the daddy long-legs spider's behavior in nature, as described in the next section.

## 3.3 The proposed PGO-DLLA algorithm

In AODV routing protocol, each node has a routing table which includes the information such as; hop count, destination sequence number (DSN), life time, source IP address. PGO-DLLA have three routing tables; the first table (L1) contains a source sequence number (SSN), destination sequence number (DSN) and lifetime of the leg (LTL1). The second table (L2) contains SSN, DSN, and the force (F). The third table is the routing table that contains all a routes discovery (RD), current route discovery (CRD), life time (LT), and the best route (BR) to destination node. Figure 1 illustrates the PGO-DLLA routing tables.

| L1 | L2 | Routing Table |
|---|---|---|
| SSN<br>DSN<br>LTL1 | SSN<br>DSN<br>F | RD<br>CRD<br>LT<br>BR |

Figure 1: PGO-DLLA routing tables.

The route discovery in PGO-DLLA is shown in Figure 2. The spider sends an agent (L1), to neighboring nodes to discover the route to the destination (prey).

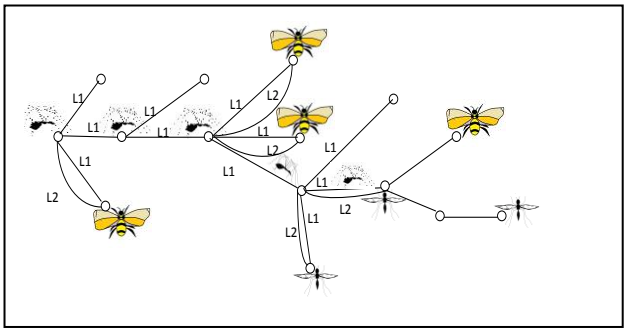



Figure 2: The route discovery in PGO-DLLA.

After broadcasting legs to all neighbor nodes, the spider (source) waits for a lifetime (LT) for receive (L2), if source receives L2 that means this node has a route to the destination or it is a destination. Then, the source node evaluates all route reply that comes from neighboring nodes using (5), to find the best move and select the next path. The Newton second law is computed the force. According to [18] Newton second law is stated as "The vector sum of the forces on an object is equal to the total mass of that object multiplied by the acceleration of the object". (2) shows the original Newton second law.

$$F_{net} = ma \tag{2}$$

Where, *m* is the mass, *a* is the acceleration where can be calculated also by Newton second law (3).

$$a = \left(F_{net} / m\right) \tag{3}$$

Depending on Hook's law [14] that is stated "The force exerted by the spring which is proportional to the length of stretch or compression of the spring and opposite in direction to the direction of the stretch or the compression". (4) shows the original Hook's law.

$$F = -kx \tag{4}$$

Where : K is constant, X is displacement. By replace the (3) by (4) we get the acceleration equal to (5).

$$a = -\left(\frac{k}{m}\right)x \tag{5}$$

We suppose that m equals to DSN, and K is constant number which sets 0.1.

## 3.4 Solution representation

The PGO-DLLA algorithm has one main goal ( shortest secure path ). The main goal can be achieved by using objective function that includes two sub goal; shortest path and secure path. The Shortest Secure path in PGO-DLLA from source to destination can be calculated by the following process Figure 3:

Step 1: Distribute one agent to every node that is a central station to its neighbors, and this is done by checking the table of each node separately.

Step 2: For each agent simultaneously (applied at same time).

Step 3: Create two tables for each agent

a) The distances table which represented the distance between agent and neighbor nodes.

b) The acceleration table which represented the evaluation function for agent to choose best path.

Step 4: Find the result of evaluation function for agent using (6).

$$\alpha = \frac{kx}{m} \tag{6}$$

Step 5: Create an ascending table for the (α) values (*ListMin*).

Step 6: Calculated the value of threshold as (7).

$$Th_{Dynamic} = \frac{kx}{DSN(6\%)} \tag{7}$$

Step 7: For ListMin (node)
If ListMin (node) <= $Th_{Dynamic}$
select Path
Exit For
else
delete Path from routing table

Step 8: Next For (new node)

Step 9: Stop

Figure 3: Pseudo code of PGO-DLLA.

An example of the route discovery in PGO-DLLA is shown in Figure 4, in this figure the source A send requests to each neighbor node (B, C and D) to discover a route to the destination. The neighbor node (B and D) are replying to source A. The source A will evaluate the node B and D separately using (5). Source Node A decided to choose the main value that less than the threshold which in this example, source A choose node B as Best route and secure at the same time.

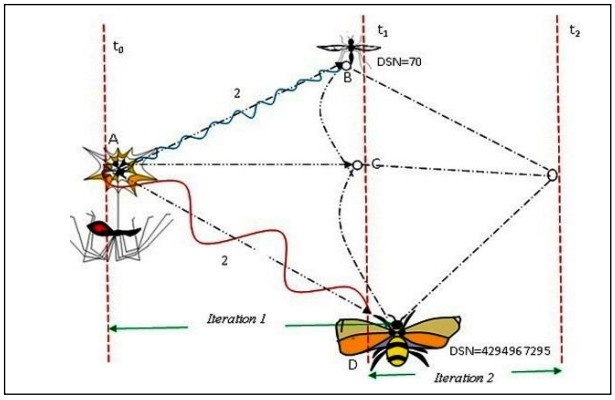



Figure 4: Example of the route discovery in PGO-DLLA.

# 4 Solution scenarios and parameters

We used NS2 simulator, version 2.33 [19], to conduct simulation scenarios in order to determine the efficacy and accuracy of our AODV routing protocol. We use the traffic rate and mobility models similar to parameters setting in simulation model that reported in [17]. The traffic sources have a continuous bit rate (CBR). The mobility model is the random waypoint model. The map area uses a square 800×800 field with 50 nodes. The pause time varies (between 10 and 100 sec.). The simulation were run 40 times for each scenario (1–4).

## 4.1 Experimental results

Simulation 1 tests the original AODV, simulation 2 tests the black hole AODV, simulation 3 tests the AntNet algorithm [20], [21], and simulation 4 tests the proposed PGO-DLLA for discovering the shortest secure path. The parameters for simulations 1–4 are shown in Table 2.

## 4.2 Performance metrics

Four performance indicators are used to measure the performance of the proposed PGO-DLLA, the standard AODV, the black hole AODV (BAODV) and AntNet. The details of these performance metrics are as follows:

- The packet delivery ratio (*PDR*) is the percentage of data packets sent by the source that are received by the destination. A larger packet delivery ratio indicates better protocol performance. (8) shows how the packet delivery ratio is computed:

$$PDR = \frac{\text{Number of Data Packets Received}}{\text{Number of Data Packets Sent}} \quad (8)$$

- Packet loss (*PL*) is the percentage of packets that are lost during the simulation. A lower packet loss rate indicates better protocol performance. (9) shows how packet loss is computed:

$$PL = \text{Packets Sent - Packets Received} \quad (9)$$

- The end-to-end delay (*EtoE*) is the average time taken for data packets to reach the destination. Only the data packets that are successfully addressed and delivered are counted. A lower end- to-end delay indicates better performance. (10) shows how the end-to-end delay is computed:

$$EtoE = \frac{\sum \text{Arrival Time - Transsmission Time}}{\sum \text{Connections}} \quad (10)$$

- Throughput (*TH*) is the number of packets received per unit of simulation time. A higher throughput value indicates better protocol performance. (11) shows how throughput is computed:

$$TH = \frac{\sum \text{Packets Received}}{\text{Simulation Time}} \quad (11)$$

## 4.3 Results of the comparison of PGO-DLLA with AntNet and discussion

For these scenarios, the pause time was varied from 0 to 100 sec., as shown in the parameters for scenarios 3 and 4 in Table 2. In Figure 5-a, the PDR for PGO-DLLA was better than the PDR for the AntNet algorithm for most sets of pause times. This is because of the new routing characteristics of the proposed algorithm, which finds the shortest route to the destination node with the smallest number of hops.

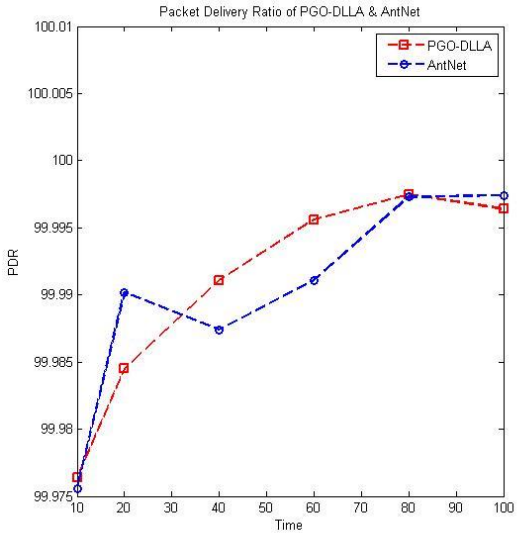
Generally, when the algorithm selects a route based on a smaller hop count, it chooses the shortest path to the destination node and thus avoids some potential link failures. For this reason, the average end-to-end delay may decrease [22]. In Figure 5-b, the value of the EtoE for PGO-DLLA was slightly higher than for the AntNet algorithm. One reason for this is the calculation that is required to find a new route in order to avoid attacks.

Throughput measures the number of packets from the source that are received by the destination node. If any delay occurs as the result of complex routing or updating the route, the throughput will be decreased [23].

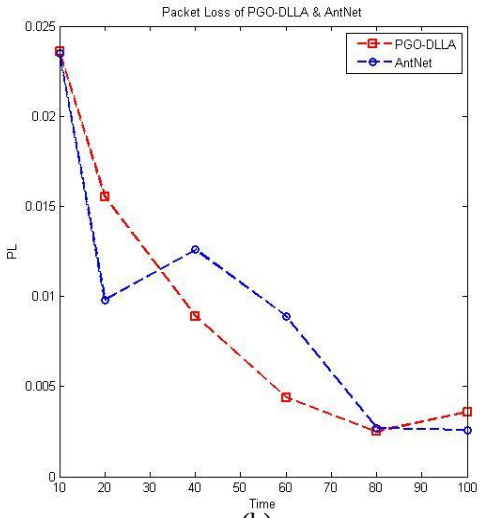
As shown in Figure 5-c, PGO-DLLA has better throughput than the AntNet algorithm during the first four time periods (t = 10, 20, 30,40), and, the throughput of the AntNet algorithm then becomes better. Nevertheless, the throughput of PGO-DLLA and the AntNet algorithm both increase across time.

Figure 5 (a, b, and c) shows a distinctive peak in AntNet graphs, the reason behind that is the using of two different routing discovery in AntNet and PGO-DLLA algorithms. Specifically, AntNet algorithm has a multipath routing that helps it to avoid the link fails, while PGO-DLLA has multi agent's strategy that takes some period (from 10 to 20 Sec.) to configure the routing tables. Hence, some distinctive peaks have been appeared in the beginning of executing AntNet compared against PGO-DLLA.

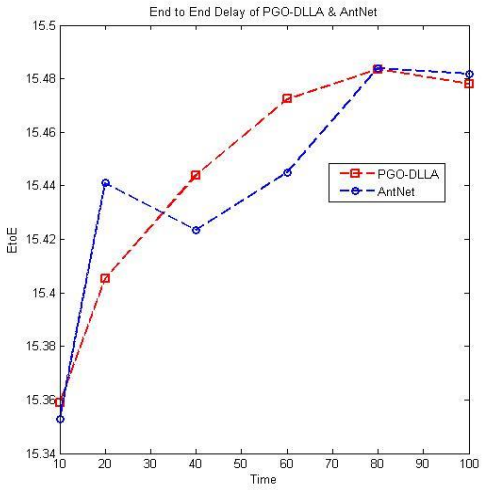
In some cases where intermediate nodes make routing decisions, such as in self-adaptive algorithms, the nodes update the routing after each iteration. In such algorithms, the routing discovery is not done by the source node, and most of these algorithms are designed to work in dynamic environments. As a result, the packet dropping rate will increase, which results in an increased packet loss rate. However, PGO-DLLA has a more stable packet loss rate than the AntNet algorithm because of its special way of routing to the destination node, as shown in Figure 5-d.



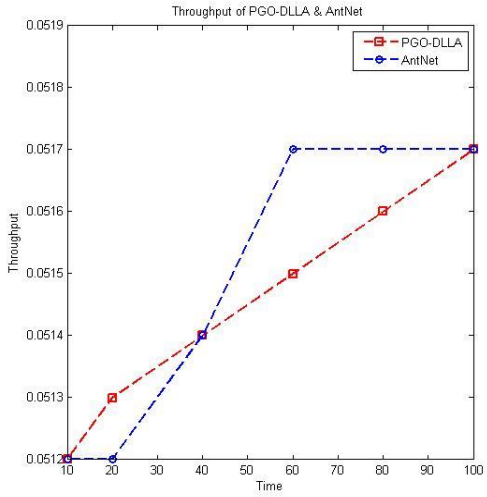

(a)




(b)




(c)




(d)

Figure 5: The results of compression of PGO-DLLA and AntNet; (a) PDR, (b) PL, (c) EtoE, (d) TH.

## 4.4 Results of the comparison of PGO-DLLA with AODV and BAODV and discussion

Even though the rate of throughput is small, because the pause time equals zero (continuous motion), the PDR may be not affected [24]. In such a situation, the new proposed algorithm has more than one strategy to ensure that all packets are received by the destination nodes. In Figure 6-a, we can see some decrease in the PDR for BADOV and standard AODV, as the effect of black hole attacks from a malicious node. In contrast, the PDR rate for PGO-DLLA increases, because of its strategy to avoid black hole attacks while retaining the shortest path to the destination node.

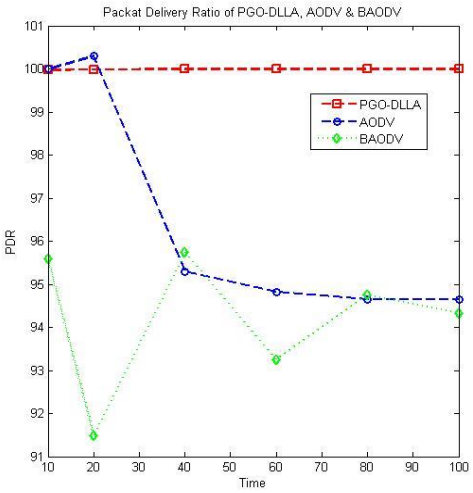
Figure 6-b shows a comparison of PGO-DLLA, BADOV, and standard AODV with respect to the average end-to-end delay. In this figure we can see that PGO-DLLA has a lower rate of delay, which is because

(d)

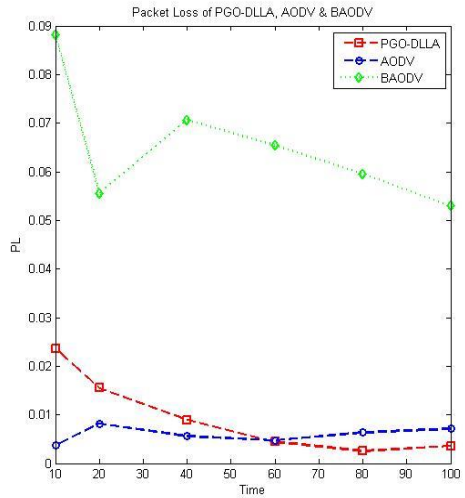
of its strategy to change the route when it is broken as a result of misbehaving nodes. In contrast, the average end-to-end delay for BADOV increases, as the effect of black hole attacks.

Figure 6-c shows a comparison of PGO-DLLA, BADOV, and standard AODV with respect to throughput. In this figure, we can see that PGO-DLLA has a higher throughput, because it can avoid dropping packets as a result of black hole attacks and change the route to the destination if it finds any disconnection. In contrast, the throughput for BADOV is very low, which is the effect of having black hole attacks without any strategy to avoid the attacks.

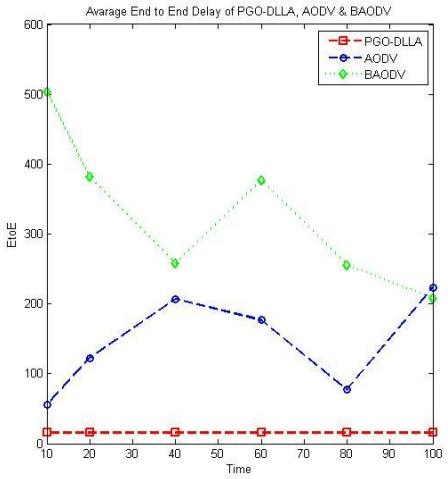
Figure 6-d shows a comparison of PGO-DLLA, BADOV, and standard AODV with respect to the rate of packet loss. In this figure, we can see that BADOV has a higher loss rate, as the result of black hole attacks. In contrast, PGO-DLLA has a very low loss rate, which is very close to that of the standard AODV.



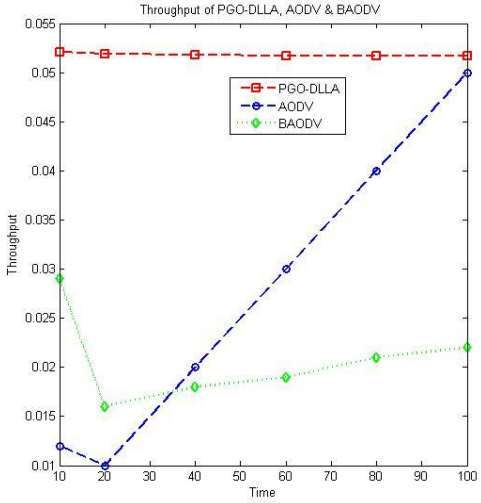

(a)




(b)




(c)




(d)

Figure 6: The results of compression of PGO-DLLA with standard AODV and Black Hole AODV; (a) PDR, (b) PL, (c) EtoE, (d) TH.

# 5 Conclusions

This paper proposes a defense mechanism against a cooperative black hole attack in a MANET that relies on the AODV routing protocol. The new method is called the PGO-DLLA protocol, modifies the standard AODV and optimizes the routing process. The idea inspired by a spider called daddy long-legs is a new technique for finding suspicious nodes and avoiding black hole attacks. As a swarm algorithm, the PGO-DLLA can consolidate the routing mechanism. Some changes are made in the routing tables to store the shortest and secure path from source to destination node. The main objective in this method is to avoid black hole attacks without causing delays in the routing protocol. The experimental results show that PGO-DLLA is able to improve the performance of the network with respect to most of the performance metrics examined. For future work, we plan to examine the enforcement of additional complex

attacks and the latest routing. The PGO-DLLA algorithm could not work on real maps directly, some adjustments would be needed (for instance, we need to adjust the distances between the nodes to the real distances among cities in the real maps, and we need to calculate a risk level value rather than the destination sequence number DSN).

# References


[1] E. Bechinski, D. Schotzko, and C. Baird, "Homeowner guide to spiders around the home and yard," 2010.

[2] A. E. Wignall and M. E. Herberstein, "Male courtship vibrations delay predatory behaviour in female spiders.," *Sci. Rep.*, vol. 3, p. 3557, Jan. 2013.

[3] F.-H. Tseng, L.-D. Chou, and H.-C. Chao, "A survey of black hole attacks in wireless mobile ad hoc networks," *Human-centric Comput. Inf. Sci.*, vol. 1, no. 1, p. 4, 2011.

[4] J. Burbank, P. Chimento, B. Haberman, and W. Kasch, "Key Challenges of Military Tactical Networking and the Elusive Promise of MANET Technology," *IEEE Commun. Mag.*, vol. 44, no. 11, pp. 39–45, Nov. 2006.

[5] C. Perkins and E. Royer, "Ad-hoc on-demand distance vector routing," in *Proceedings WMCSA'99. Second IEEE Workshop on Mobile Computing Systems and Applications*, 1999, pp. 90–100.

[6] L. Tamilselvan and V. Sankaranarayanan, "Prevention of Co-operative Black Hole Attack in MANET," *J. Networks*, vol. 3, no. 5, pp. 13–20, May 2008.

[7] H. Nakayama and S. Kurosawa, "A dynamic anomaly detection scheme for AODV-based mobile ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 58, no. 5, pp. 2471–2481, 2009.

[8] S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour, and Y. Nemoto, "Detecting blackhole attack on AODV-based mobile Ad Hoc networks by dynamic learning method," *Int. J. Netw. Secur.*, vol. 5, no. 3, pp. 338–346, 2007.

[9] X. Zhang, Y. Sekiya, and Y. Wakahara, "Proposal of a method to detect black hole attack in MANET," in *Proceedings - 2009 International Symposium on Autonomous Decentralized Systems, ISADS 2009*, 2009, pp. 149–154.

[10] Y. Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks," in *Proceedings of the 6th annual international conference on Mobile computing and networking - MobiCom '00*, 2000, pp. 275–283.

[11] R. Mitchell and I.-R. Chen, "A survey of intrusion detection in wireless network applications," *Comput. Commun.*, vol. 42, pp. 1–23, Apr. 2014.

[12] K. I. Ghathwan, A. R. Yaakub, and R. Budiarto, "EAODV: A*-Based enhancement ad-hoc on demand vector protocol prevent black hole attacks," *J. Ilmu Komput. dan Inf.*, vol. 6, no. 2, pp. 45–51, 2013.

[13] K. I. Ghathwan and A. R. B. Yaakub, "An Artificial Intelligence Technique for Prevent Black Hole Attacks in MANET," in *Recent Advances on Soft Computing and Data Mining*, Springer International Publishing, 2014, pp. 121–131.

[14] S. Horibe, "Robert Hooke, Hooke's Law & the Watch Spring," 2011.

[15] C. Benjamin, *Laser-Tissue Interactions*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, p. 218.

[16] A. Sherif, M. Elsabrouty, and A. Shoukry, "A Novel Taxonomy of Black-Hole Attack Detection Techniques in Mobile Ad-hoc Network (MANET)," in *2013 IEEE 16th International Conference on Computational Science and Engineering*, 2013, pp. 346–352.

[17] C. Perkins, E. Royer, S. R. Das, and M. K. Marina, "Performance comparison of two on-demand routing protocols for ad hoc networks," *IEEE Pers. Commun.*, vol. 8, no. 1, pp. 16–28, 2001.

[18] G. L. Lucas, F. W. Cooke, and E. A. Friis, *A Primer of Biomechanics*. New York, NY: Springer New York, 1999.

[19] A. Bright, J. R. Waas, C. M. King, and P. D. Cuming, "Bill colour and correlates of male quality in blackbirds: An analysis using canonical ordination," *Behav. Processes*, vol. 65, pp. 123–132, 2004.

[20] G. Di Caro and M. Dorigo, "AntNet: Distributed Stigmergetic Control for Communications Networks," *J. Artif. Intell. Res.*, vol. 9, pp. 317–365, May 1998.

[21] H. Huang, H.-B. Xie, J.-Y. Guo, and H.-J. Chen, "Ant colony optimization-based feature selection method for surface electromyography signals classification.," *Comput. Biol. Med.*, vol. 42, no. 1, pp. 30–8, Jan. 2012.

[22] C. Sarr, I. Guérin-Lassous, and others, "Estimating average end-to-end delays in IEEE 802.11 multihop wireless networks," 2007.

[23] P. Li, Y. Fang, and J. Li, "Throughput, delay, and mobility in wireless ad hoc networks," in *INFOCOM, 2010 Proceedings IEEE*, 2010, pp. 1–9.

[24] S. K. Tiong and H. S. Jassim, "EMNet: Electromagnetic-like Mechanism based routing protocol for Mobile ad hoc network," *Trendas Appl. Sci. Res.*, vol. 7, no. 11, pp. 881–900, Nov. 2012.