Improved Security Particle Swarm Optimization (PSO) Algorithm to Detect Radio Jamming Attacks in Mobile Networks

Ahmad K. Al Hwaitat[1], Mohammed Amin Almaiah[2], Omar Almomani[3], Mohammed Al-Zahrani[4]
Rizik M. Al-Sayed[5], Rania M.Asaifi[6], Khalid K. Adhim[7], Ahmad Althunibat[8], Adeeb Alsaaidah[9]
Faculty of King Abdullah II School for Information Technology, The University of Jordan, Amman, Jordan[1, 5, 7]
Faculty of Computer Sciences and Information Technology, King Faisal University, Al-Ahsa, Saudi Arabia[2, 4]
Faculty of Information Technology, The World Islamic Sciences & Education University, Amman, Jordan[3, 9]
Faculty of Business, The University of Jordan, Amman, Jordan[6]
Department of Software Engineering, Al-Zaytoonah University of Jordan, Amman, Jordan[8]

***Abstract*— Jamming attack is one of the most common threats on wireless networks through sending a high-power signal to the network in order to corrupt legitimate packets. To address Jamming attacks problem, the Particle Swarm Optimization (PSO) algorithm is used to describe and simulate the behavior of a large group of entities, with similar characteristics or attributes, as they progress to achieve an optimal group, or swarm. Therefore, in this study enhanced version of PSO is proposed called the Improved PSO algorithm aims to enhance the detection of jamming attack sources over randomized mobile networks. The simulation result shows that Improved PSO algorithm in this study is faster at obtaining the location of the given mobile network at which coverage area is minimal and hence central compared to other algorithms. The Improved PSO as well was applied to a mobile network. The Improved PSO algorithm was evaluated with two experiments. In the First experiment, The Improved PSO was compared with PSO, GWO and MFO, obtained results shown the Improved PSO is the best algorithm among others to fine obtain the location for jamming attack. In Second experiment, Improved PSO was compared with PSO in mobile network environment. The obtain results prove that Improved PSO is better than PSO for obtaining the location in mobile network where coverage area is minimal and hence central.**

Keywords—Jamming attacks; Mobility; PSO; mobile networks; attacked detection; network security

I. Introduction

Wireless sensor networks are especially sensitive to Denial of Services Attacks (DoS) [22] such as Jamming attacks [1]. The DoS attacks have a huge chance of attacking in the wireless sensor networks for the services provided by the network. In this case, the network performance would be decreased since the detection of the denial of service attack is difficult. However [23][25], wireless sensor networks are exposed to different forms of attacks such as data integrity and confidentiality[24]attacks that include Denial of Service (DOS) attack, power consumption related attacks such as Denial of Sleep attack and service availability and bandwidth consumption related attacks, which includes flooding attacks and Jamming attacks.

One of the most common types of DOS attacks on wireless sensor network is jamming attack. Jamming attack happens when attackers send a high-power signal in order to generate interference and avoid correct reception of legitimate packets. Jamming attack at the wireless network consisted of sending a high-power signal to the network in order to corrupt legitimate packets.

The main purpose of jamming attack is to disrupt the signal transmission during the communication of the users the jamming device [19] intentionally emits the electromagnetic energy. It is considered as one of the main adversarial threat and it degrades the performance of the network. By continuously transmitting, the jamming signals the attackers would able to interfere between the users' communication. In addition, the jammer could be used to prevent the traffic in the wireless medium. Within a certain radius, the jammer could able to block all the radio communication on any device which uses the radio signal frequencies for transmission.

Wireless sensor networks are mostly susceptible to Jamming attacks due to limited resources such as processing capability, memory and insecure transmission medium [18], [20]. To address the problem of how to enhance the security of wireless networks from jamming attacks, several methods and algorithms have been developed. For example, Le Wang and Alexander [17] developed a new method to detect jamming attacks and determine the type of jamming attack using signal strength and packet delivery ratio mechanisms. The main weakness of this method was not able to detect the source of jamming. Ghosal [1] applied the spread spectrum (SS) method to detect the jamming attacks through spreading data being transmitted across the frequency spectrum. This method has many limitations such as inefficient, complexity and more costly in terms of computation as compared to other methods.

Other approaches focused on detecting the jamming attacks in mobile networks. Muraleedharan and Osadciw [4] proposed a novel method to detect jamming attacks using ANT system. The main purpose of this method was to analyze the DOS attack and predict the type of DOS attacks in order to identify the best defense mechanism. This method helped in increasing the reliability of quality of service of wireless sensor network.

Quintana [5] developed a hybrid method by combining Particle Swarm Optimization (PSO) and ANT to mitigate attacks using Time-Hopping Spread-Spectrum system. In the same way, Ramírez-Mireles [6] proposed approach based on two functions, Private Key Based Time Hopping and Selected Diversity Based Time Hopping in order to confuse the jammer and reduce its ability to target the carrier frequency being transmitted by the node.

Due to some weaknesses of existing methods of jamming detection, where most of them are unable to detect the sources of jamming attacks. Therefore, this paper attempts to fill the research gap by proposing an algorithm called the improved PSO algorithm in order to enhance the detection of jamming noise by determining the locations and sources of jamming attacks in mobile network. Then, we evaluated the improved PSO by conducting two experimental tests. In first experiment, the Improved PSO algorithm was compare with PSO, Grey Wolf Optimizer (GWO) and Moth-Flame Optimization (MFO) with different test function. All algorithms were executed on a randomized particle swarm using a series of test functions. In the second experiment, The Improved PSO and PSO algorithms are performed on a randomized mobile network in order to find the optimal location for the jamming system to be positioned [21].

The rest of this paper is organized as follows: Section 3 contains the related work, Section 3 describes the Proposed Improved PSO and its Application to Detect Jamming Attack then it describes the Mathematical model for Detection of Jamming. Finally, Sections 4 and 5 contain the experimental results and the conclusion.

II. Related Works

In the literature, there are several methods that have been developed to detect the jamming attack in wireless sensor networks. In this section, we overviewed some of existing methods that addressed this problem. Most of these studies focused on detecting the jamming attack executions and prevention of jamming attacks. For instance, Houssaini M.A.E et al. [7], proposed a new method for detecting jamming attacks in mobile networks using statistical process control (SPC). The SPC method has been applied to the packet drop ratio (PDR) which refers to the number of dropped data packets to the total of data packets sent in a mobile network. Another method developed by Chaturvedi P. and Gupta K. [8], which aimed to detect and prevent several types of Jamming attacks in wireless networks. The proposed method discussed about jamming attacks in general and how they can be physically implemented to attack a wireless network. This discussion is then followed by a description of a variety of both detection and prevention techniques implemented against jamming attacks. Chaturvedi P. and Gupta K. [9] presented another method for Jamming attacks and prevention techniques using Honeypots in wireless networks. The method was focused on jamming situations where the jammer is a part of the given network in the situation, i.e., which have internal knowledge of the network protocol specifications, thus making them even more difficult to detect. This study continues further to explain the four jamming models that a jammer can use to attack a wireless network.

Sari A. and Necat B. [10] proposed a new method using Unified Security Mechanism (USM) to enhance the security of mobile Ad-Hoc Networks against Jamming attacks. This method explained explains how jamming attacks can occur through the MAC (Medium Access Control) layer of a mobile ad-hoc network and how their proposed method to prevent jamming attacks can be used in this layer. There are different coordination mechanisms that the method implements in this layer, mainly the Point Controller Functions (PCF) and RTS/CTS (Request to Send/Clear to Send) mechanisms. In the same way, Xu W. et al. [11], proposed two detection methods for detecting Jamming attacks in wireless networks. The first method checks the signal strength of the data packets being delivered in the wireless network, and the second one consistently checks similar local measurements. Balogun V. and A. Krings [12] proposed a method for jamming attacks inflicted on cognitive radio networks through fault-model classification, followed by a prevention technique designed specifically for fault models.

Jamming Probability and Network Channel Access Probability in Wireless Sensor Networks, by Chowdary and Ali [13], described in detail how jammers depend on the knowledge of details of the network, like network channel access probability, to attack it, and how the network depends on the knowledge of details of the jammer, like the jamming probability, to be able to detect it. Two case are experimented on – first, an ideal situation where both the network and the jammer have all the necessary information on each other to execute their actions, and second, a situation where only the jammer does not have the information it needs to execute an attack. Effect of Jamming Attack in Mobile Ad Hoc Environment, by Popli P. and Raj P. [14], gives an in-depth descript of how jammers, using radio waves, disrupt signals being sent to or from a mobile node. It then continues to specifically focus on differentiating between the performance of mobile ad-hoc networks with and without a jamming device in their vicinities. Using IEEE standards, a mobile ad-hoc network is simulated and tested for performance with and without a jammer and the results are compared. Packet-Hiding Methods for Preventing Selective Jamming Attacks, by Pavani G. [15], begins with an explanation of selective jamming attacks, and how they are an improved version of jamming attacks, in the sense that they can target data signals of importance. Moreover, these types of attacks stay active for very short periods of time, and hence are harder to detect. Two situations are then discussed – an attack on the TCP layer of a network and an attack on the routing of a network – followed by a discussion of three proposed schemes to prevent these attacks.

A. Particle Swarm Optimization (PSO)

This algorithm starts with a group of entities with random locations, calculates their individual location-based fitness values and then searches for the entity with optimal fitness value of the group, which can be called the global best value [3]. Another optimal fitness value that each entity keeps track of is the best fitness value the node has had so far, which can be called the local best value [26].

After the two optimal values are calculated for all entities, their positions are updated with the following equations [1] and [2]:

$$\begin{cases} \vec{v}_i^{(t)} = \vec{v}_i^{(t-1)} + \varphi_1(p_l - \vec{x}_i^{(t-1)}) + \varphi_2(p_g - \vec{x}_i^{(t-1)}) \\ x_i^{(t)} = x_i^{(t-1)} + \vec{v}_i^{(t)} \end{cases} \quad (1)(2)$$

Where X is the position of the current entity being analysed, Pl is the position of the entity with the local best fitness value, Pg is the position of the entity with the global best fitness value, I is the current dimension being analysed, t is the current iteration and phi1 and phi2 are learning factors (usually 0 to 1 and user defined).

Depending on the situation the algorithm is applied to, the user can either define the number of iterations to run the algorithm for or the required optimal value to attain. The pseudo code for this algorithm is given below:

```
    for every iteration
for every dimension
    Return back the entities that go beyond the
    boundaries of the search space;
    end for

    for every entity
    calculate the current fitness value;

    if current fitness value is better than local best
    fitness value
    local best fitness value = current fitness value;
    position of entity with local best fitness = position of
    current entity;
    end

    if current fitness value is better than global best
    fitness value
    global best fitness value = current fitness value;
    position of entity with global best fitness = position
    of current entity;
    end
    end for

    for every entity
        use equations 1 and 2 to calculate the
    change in position for each dimension
            and update the position of each
    particle accordingly;
    end for
    end
```

After many iterations, eventually all entities the swarm will reach an optimal fitness value and associated position, i.e., the optimal fitness position.

The pseudo code for the application of the original PSO to a mobile network is given below:

```
    for every iteration
    for every dimension
    Return back the nodes that go beyond the
    boundaries of the search space;
    end for
    for every node
    for every other node
  calculate radial distance between current node and other
                         node and
calculate the corresponding circular area;
    end for

    Coverage area of the current node = maximum of
    all circular areas computed;

    if current coverage area is smaller than local
    minimum coverage area
    local minimum coverage area = current coverage
    area;
    position of node with local minimum coverage area
    = position of current node;
    end

    if current coverage area is smaller than global
    minimum coverage area global minimum coverage
    area = current coverage area;position of node with
    global minimum coverage area = position of current
    node;
    end
    end for

    for every node use equations 1 and 2 to calculate
    the change in position for each dimensionand
    update the position of each node accordingly;
    end for
    End
```

III. Proposed Algorithm

A. The Improved PSO

The improved PSO algorithm aims at reducing the number of iterations required to reach the optimal fitness value. Improved PSO updated positions according to equation 3 & 4.

$$\vec{v}_i^{(t)} = \vec{v}_i^{(t-1)} + sign\left(p_l - \vec{x}_i^{(t-1)}\right) * \left(p_l - \vec{x}_i^{(t-1)}\right)^2 + sign\left(p_g - \vec{x}_i^{(t-1)}\right) * \left(p_g - \vec{x}_i^{(t-1)}\right)^2 \quad (3)$$

$$x_i^{(t)} = x_i^{(t-1)} + \vec{v}_i^{(t)} \quad (4)$$

The Improved PSO entity positions are normalized, means their position values are described in terms of fractions of the boundary lengths. As well as learning factors in Improved PSO phi1 and phi2 are assumed to be 1. Below shows pseudo code for Improved PSO algorithm.

```
For every iteration
for every dimension
Return back the entities that go beyond the boundaries of the search space
end for
        for every entity
                  calculate the current fitness value;
if current fitness value is better than local best fitness value
local best fitness value = current fitness value;
position of entity with local best fitness = position of current entity;
end
if current fitness value is better than global best fitness value
global best fitness value = current fitness value;
position of entity with global best fitness = position of current entity;
end
end for
for every entity
        use equations 3 and 4 to calculate the change in position for each dimension
                  and update the position of each particle accordingly;
end for
  end
```

Improved PSO algorithm is applied to mobile networks according to pseudo code shows below:

```
For every iteration
for every dimension
Return back the nodes that go beyond the boundaries of the search space;
end for
      for every node
                for every other node
Calculate radial distance between current node and another node and
calculate the corresponding circular area;
end for
if current fitness value is better than local best fitness value
local best fitness value = current fitness value;
position of entity with local best fitness = position of current entity;
end
if current fitness value is better than global best fitness value
global best fitness value = current fitness value;
position of entity with global best fitness = position of current entity;
end
end for
for every node
      use equations 3 and 4 to calculate the change in position for each dimension
      and update the position of each node accordingly;
end for
end
```

B. Jamming Attack Detection based on Improved PSO Algorithm

Improved PSO can detect jamming attack in mobile networks by determines location of jamming source. Fig. 1 shows steps for detecting jamming attack in mobile network based on Improved PSO.

C. Mathematical Model for Detection of Jamming Attack

Jamming devices are better designed to provide the best possible network coverage to cause harm [16]. The jamming source will be easier to find if each node's coverage area is minimized. The coverage area of each node is defined as the area of the largest circle that can be created by joining a line of radius between the node in question and the distant node. coverage area calculates in equation 5.

$$S = \max\{\pi * |xi - a|^2\} \quad (5)$$

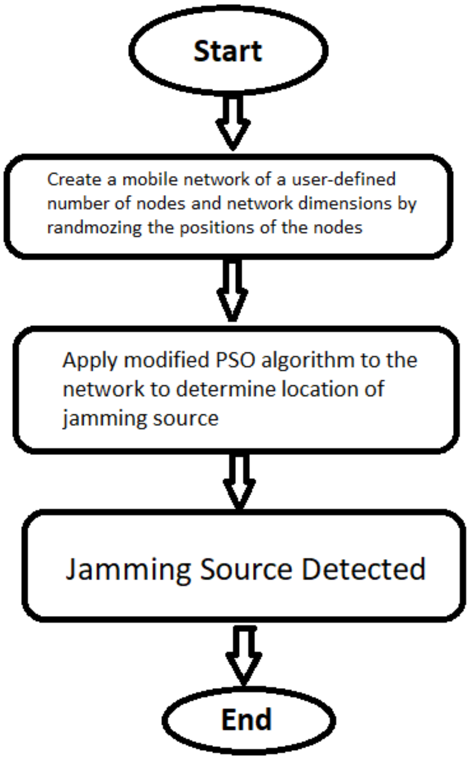

Start
Create a mobile network of a user-defined number of nodes and network dimensions by randmozing the positions of the nodes
Apply modified PSO algorithm to the network to determine location of jamming source
Jamming Source Detected
End

Fig. 1. Jamming Attack Detection based on Improved PSO.

Where α is denoted to dimensional position of the current node and i represents the position of the other node being used as well to calculate the radius between the two nodes. Coverage area for 1D, 2D and 3D calculate using equation 6,7,8, respectively.

$$\text{1D=>}xi - a \tag{6}$$

$$\text{2D=>}\sqrt{(xi - ax)^2 + (yi - ay)^2} \tag{7}$$

$$\text{3D=>}\sqrt{(xi - ax)^2 + (yi - ay)^2 + (zi - az)^2} \tag{8}$$

After calculating coverage area for a single node, its local minimal coverage area is computed and updated as in equation 9. The coverage area for every node is computed within a single iteration the global minimal coverage computed and updated as in equation 10.

$$S_{local} = Smallest\ S\ the\ current\ node\ has\ ever\ had \tag{9}$$

$$S_{min} = S_{global} = \min\{\max\{\pi * |xi - a|^2\} \tag{10}$$

Finally, the positions of all of nodes is update for single iteration according to equations 11 and 12.

$$Position\_change_i^{(t)} = Position\_change_i^{(t-1)} + sign\left(Optimal\_node\_pos_{local} - Current\_node\_pos_i^{(t-1)}\right) * \left(Optimal\_node\_pos_{local} - Current\_node\_pos_i^{(t-1)}\right)^2 + sign\left(Optimal\_node\_pos_{global} - Current\_node\_pos_i^{(t-1)}\right) * \left(Optimal\_node\_pos_{global} - Current\_node\_pos_i^{(t-1)}\right)^2 \tag{11}$$

$$Position_i^{(t)} = Positions_i^{(t-1)} + Position\_change_i^{(t)} \tag{12}$$

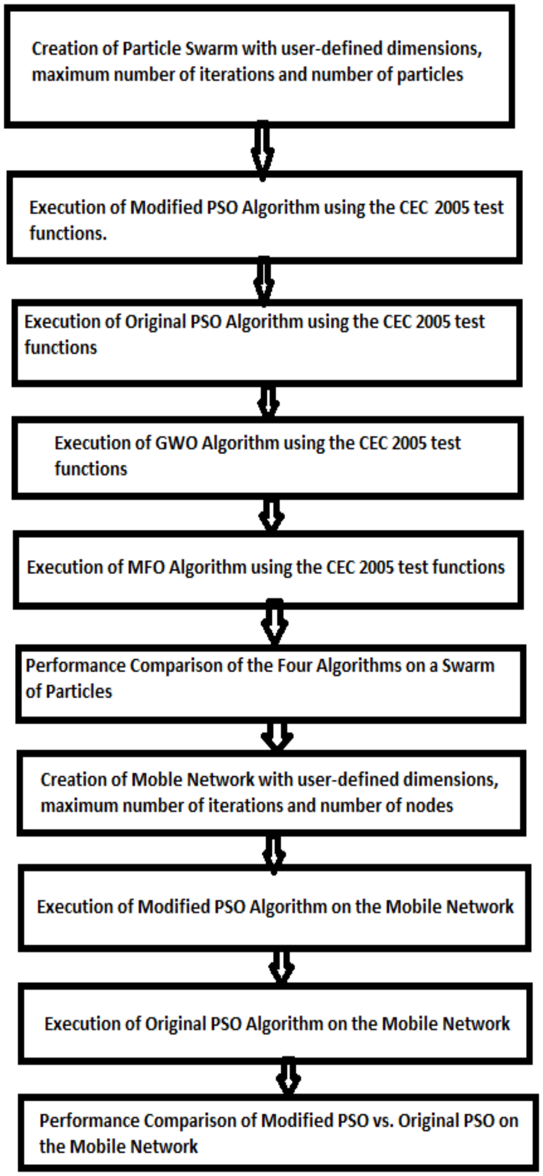
IV. Experimental Results

To evaluate the Improved PSO two experiments that were conducted. In the first experiment, the Improved PSO algorithm was compared with PSO, Grey Wolf Optimizer (GWO) and Moth-Flame Optimization (MFO) with different test function. All algorithms were executed on a randomized particle swarm using a series of test functions. In the Second experiment, The Improved PSO and PSO algorithms was performed on a randomized mobile network in order to find the optimal location for the jamming system to be positioned. Fig. 2 shows experiments procedure.

A. First Experiment Results and Discussion

Improved PSO was exam with a group of standard benchmark test functions CEC_2005 [17]. Appendix 1 shows the CEC_2005 Test Functions.

Simulations result for each test function F1 to F14 are shown in Fig. 3 to Fig. 16, respectively.



Creation of Particle Swarm with user-defined dimensions, maximum number of iterations and number of particles

Execution of Modified PSO Algorithm using the CEC 2005 test functions.

Execution of Original PSO Algorithm using the CEC 2005 test functions

Execution of GWO Algorithm using the CEC 2005 test functions

Execution of MFO Algorithm using the CEC 2005 test functions

Performance Comparison of the Four Algorithms on a Swarm of Particles

Creation of Moble Network with user-defined dimensions, maximum number of iterations and number of nodes

Execution of Modified PSO Algorithm on the Mobile Network

Execution of Original PSO Algorithm on the Mobile Network

Performance Comparison of Modified PSO vs. Original PSO on the Mobile Network

Fig. 2. Experiments Procedure.

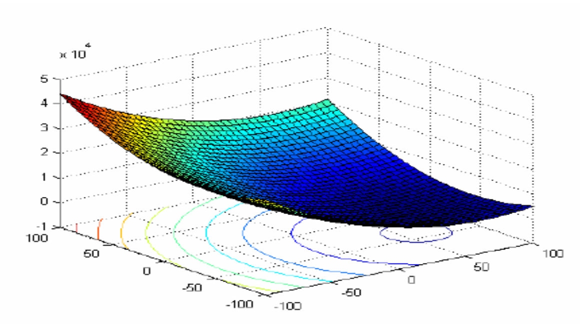


Fig. 3. F1 Test Function.

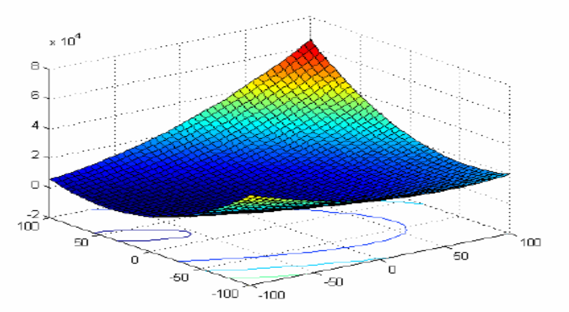


Fig. 4. F2 Test Function.

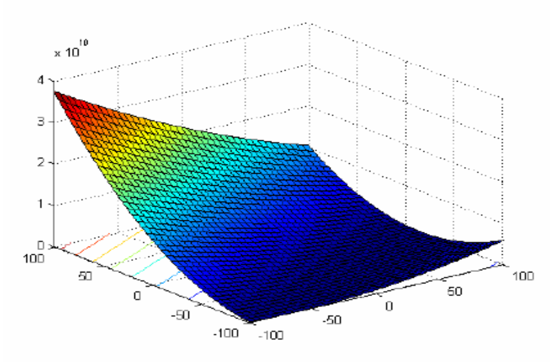


Fig. 5. F3 Test Function.

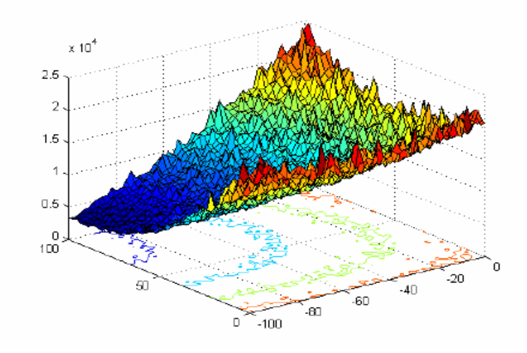


Fig. 6. F4 Test Function.

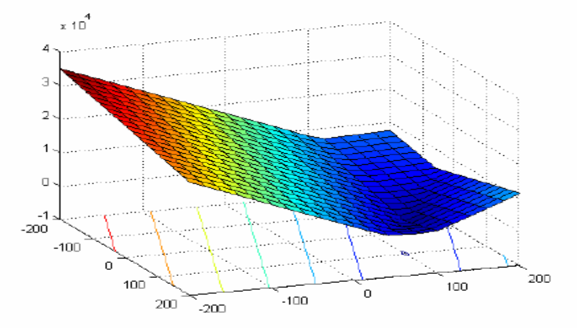


Fig. 7. F5 Test Function.

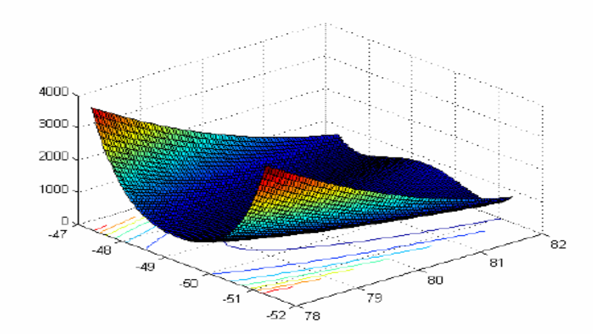


Fig. 8. F6 Test Function.

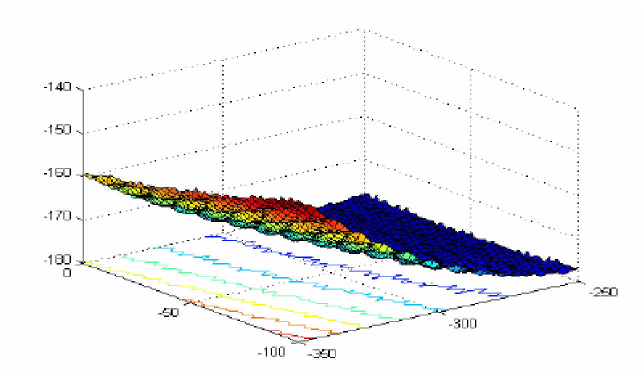


Fig. 9. F7 Test Function.

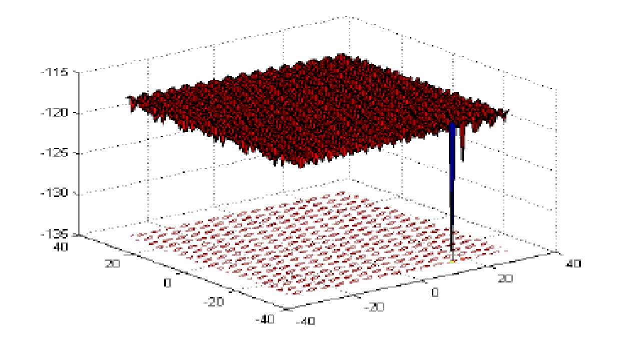


Fig. 10. F8 Test Function.

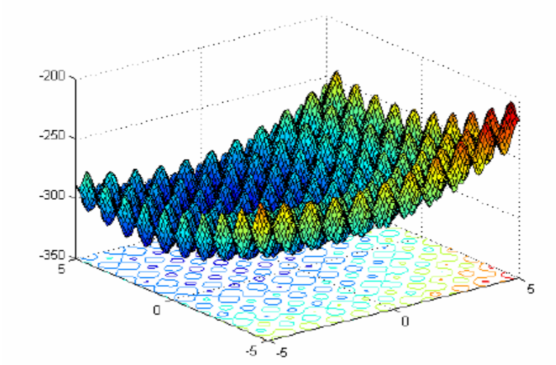


Fig. 11. F9 Test Function.

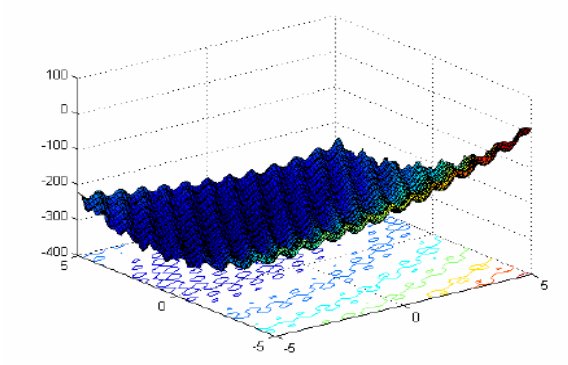


Fig. 12. F10 Test Function.

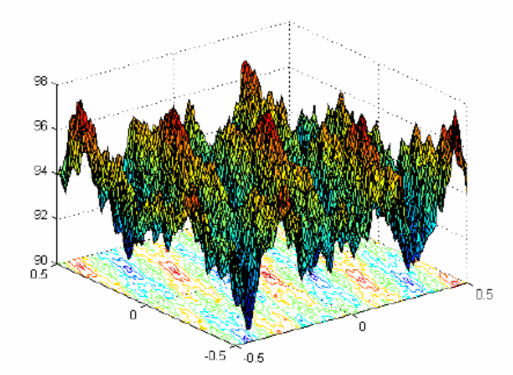


Fig. 13. F11 Test Function.

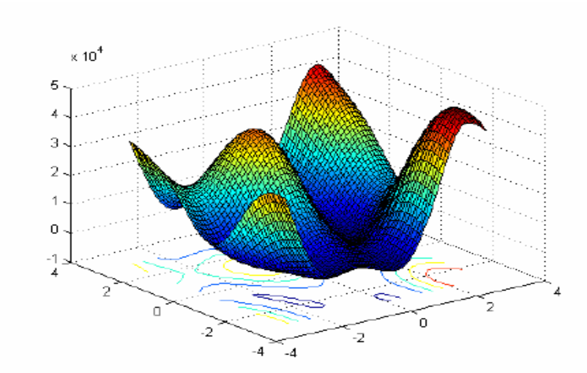


Fig. 14. F12 Test Function.

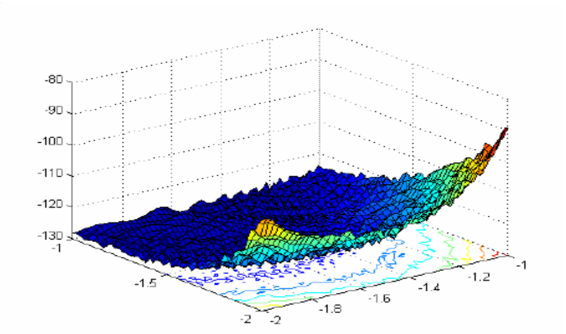


Fig. 15. F13 Test Function.

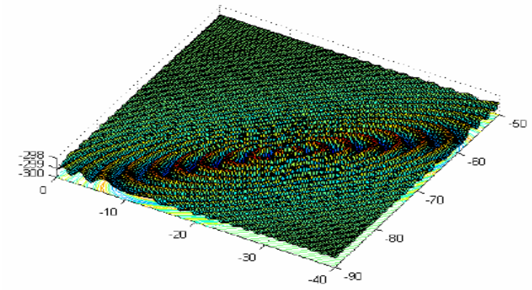


Fig. 16. F14 Test Function.

The experiment was conducted using 100 entities where location was randomized, using F1 to F14. Each algorithm was test with 100 iterations to obtain minimal fitness value of all the entities. Each experiment was run 30 times for each test function. Table I show obtained results for Improved PSO, Table II show obtained results for PSO, Table III show obtained results for GWO and Table IV show obtained results for MFO.

TABLE I. IMPROVED PSO RESULTS

Test Function	Mean	Min	Max
F1	-8000450	-8000450	-8000450
F2	-1.6E+14	-1.6E+14	-1.6E+14
F3	-4E+12	-4E+12	-4E+12
F4	-5.3E+07	-5.6E+07	-5.6E+07
F5	-549140	-550310	-550310
F6	-1.6E+15	-1.6E+15	-1.6E+15
F7	-2411.15	-8573.2	-8573.2
F8	-139.273	-139.946	-139.946
F9	-8000330	-8000330	-8000330
F10	-8000330	-8000330	-8000330
F11	89.8927	89.32279	89.32279
F12	-302026	-348217	-348217
F13	-1.3E+27	-1.3E+27	-1.3E+27
F14	-300.503	-300.55	-300.55

TABLE II. PSO RESULTS

Test Function	Mean	Min	Max
F1	-7922693.4	-8000450	-5667751
F2	-1.594E+14	-1.6E+14	-1.6E+14
F3	-4E+12	-4E+12	-4E+12
F4	-52994250	-55962633	-27981549
F5	-548960.7	-550310	-547114
F6	-1.602E+15	-1.602E+15	-1.602E+15
F7	-2415.1051	-8573.1973	-2175.9043
F8	-139.30124	-139.94577	-138.29682
F9	-8000330	-8000330	-8000330
F10	-8000330	-8000330	-8000330
F11	89.7885997	89.3227882	90.2519517
F12	-304642.2	-351107.8	-266467.1
F13	-1.282E+27	-1.283E+27	-1.281E+27

F14	-300.50356	-300.55021	-300.50002

TABLE III. GWO RESULTS

Test Function	**Mean**	**Min**	**Max**
F1	-6909926	-8000450	-4339582
F2	-1.4E+14	-1.6E+14	-9.5E+13
F3	-4E+12	-4E+12	-3.9E+12
F4	-4.5E+07	-5.6E+07	-3.2E+07
F5	-547161	-550310	-541942
F6	-1.5E+15	-1.6E+15	-6.5E+14
F7	-181486	-3240831	-5991.43
F8	-139.946	-139.993	-139.866
F9	-6856636	-8000330	-5124974
F10	-6856636	-8000330	-5124974
F11	89.1942	89.03894	89.32363
F12	-282756	-335073	-252646
F13	-1.2E+27	-1.3E+27	-8.3E+26
F14	-300.997	-300.998	-300.996

TABLE IV. MFO RESULTS

Test Function	**Mean**	**Min**	**Max**
F1	-8000450	-8000450	-8000450
F2	-1.6E+14	-1.6E+14	-1.6E+14
F3	-4E+12	-4E+12	-4E+12
F4	-5.6E+07	-5.6E+07	-5.6E+07
F5	-548071	-550310	-544810
F6	-1.6E+15	-1.6E+15	-1.6E+15
F7	-9259983	-3240831	-5021.42
F8	-97.6534	-139.993	-97.6499
F9	-8000330	-8000330	-8000330
F10	-8000330	-8000330	-8000330
F11	89.16613	89.03894	89.30676
F12	-293310	-335073	-254831
F13	-1.3E+27	-1.3E+27	-1.3E+27
F14	-300.995	-300.998	-300.94

TABLE V. COMPARISON OF IMPROVED PSO, PSO, GWO AND MFO

Test Function	**MPSO vs. PSO**	**MPSO vs.GWO**	**MPSO vs. MFO**
F1	<	<	=
F2	<	<	=
F3	=	=	=
F4	<	<	>
F5	<	<	<
F6	>	<	=
F7	>	>	>
F8	>	>	<
F9	=	<	=
F10	=	<	=
F11	>	>	>
F12	>	<	<
F13	<	<	=
F14	>	>	>

Finally, Table V present a comparison between Improved PSO, PSO, GWO and MFO in term of Average minimal fitness values.

It is observable that the Improved PSO algorithm outperformed the PSO, GWO and MFO in term of minimal fitness value. Fig. 17 to 29 show the minimal converges area value vs. iterations for all tested algorithms with respect to all test functions (F1 to F14).

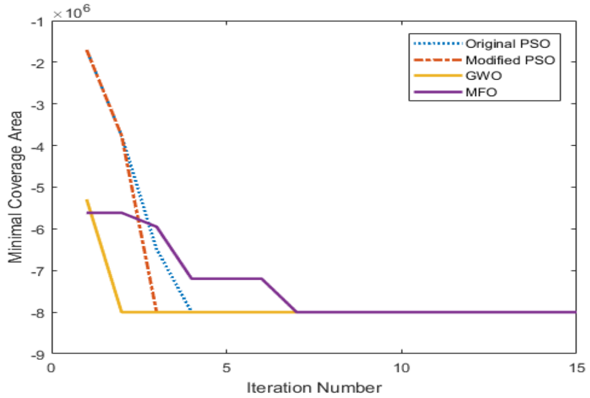


Fig. 17. Minimal Converges Area with F1.

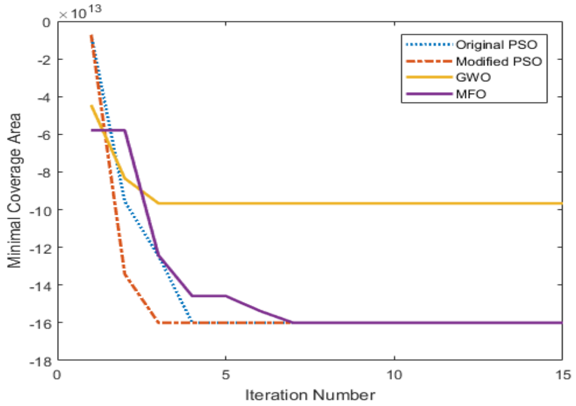


Fig. 18. Minimal Converges Area with F2.

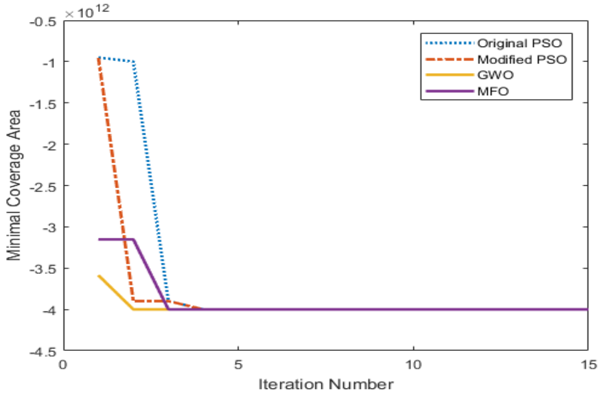


Fig. 19. Minimal Converges Area with F3.

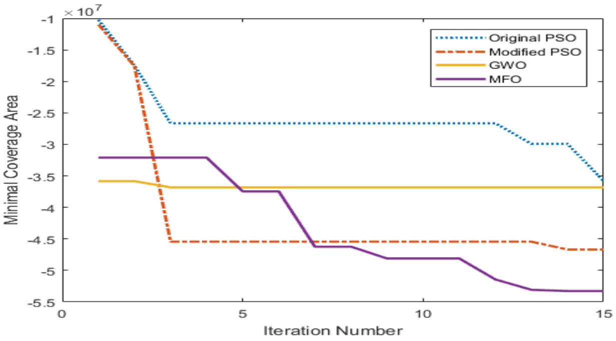


Fig. 20. Minimal Converges Area with F4.

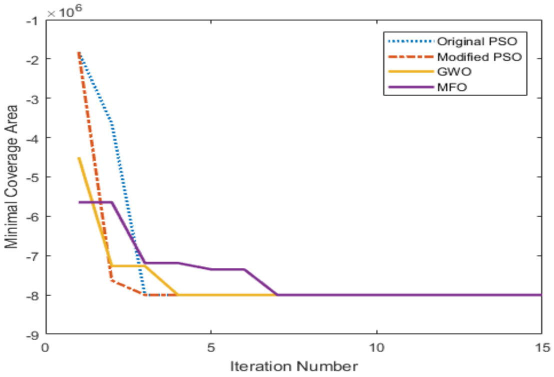


Fig. 24. Minimal Converges Area with F8.

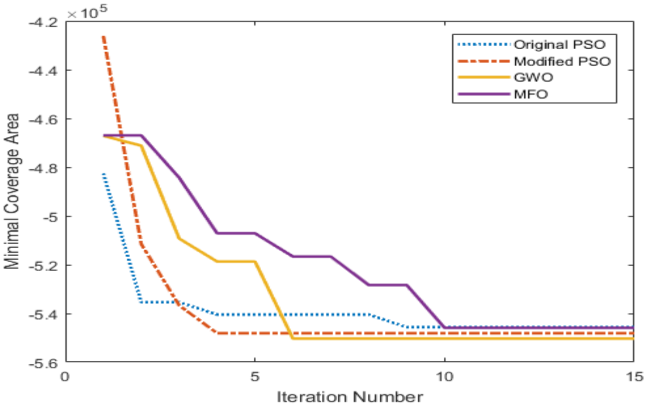


Fig. 21. Minimal Converges Area with F5.

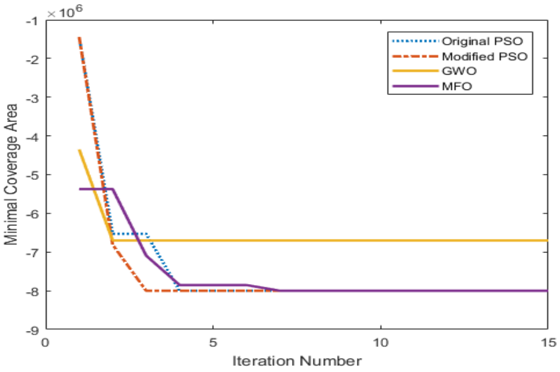


Fig. 25. Minimal Converges Area with F9.

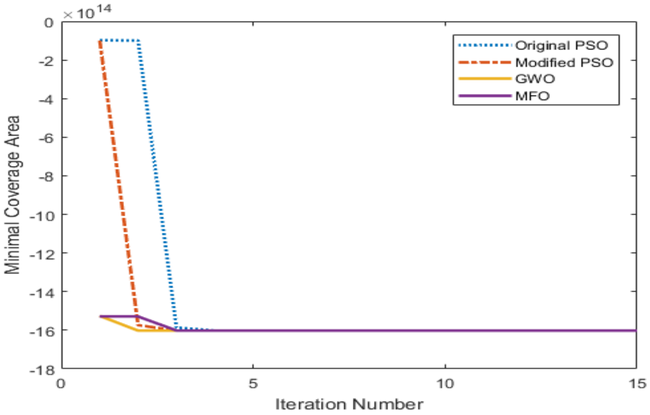


Fig. 22. Minimal Converges Area with F6.

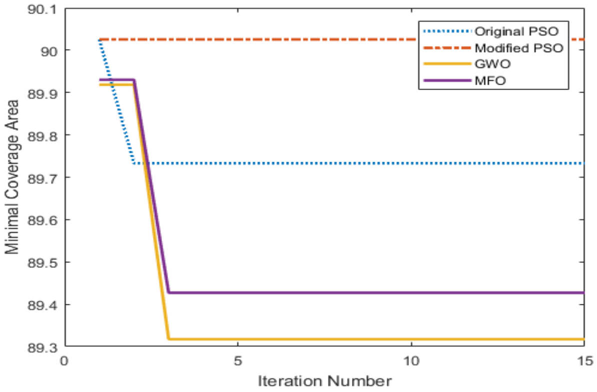


Fig. 26. Minimal Converges Area with F10.

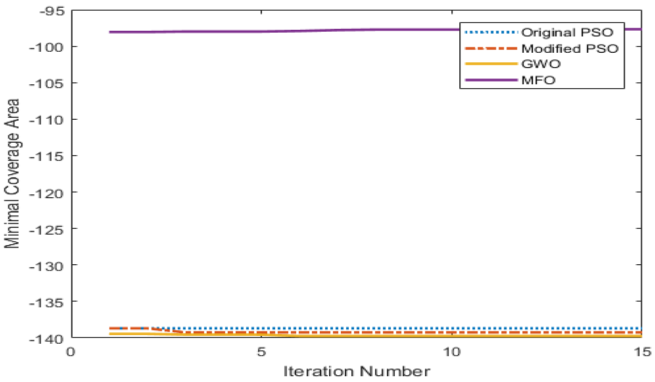


Fig. 23. Minimal Converges Area with F7.

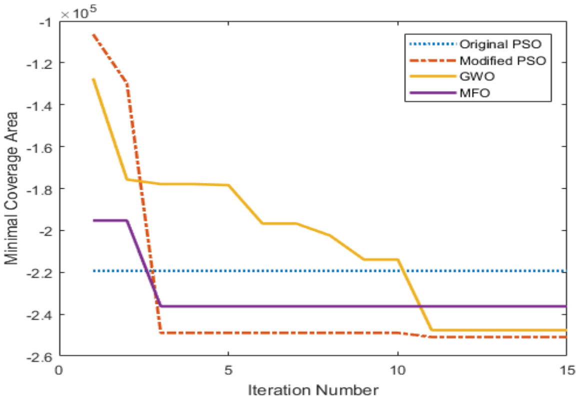


Fig. 27. Minimal Converges Area with F11.

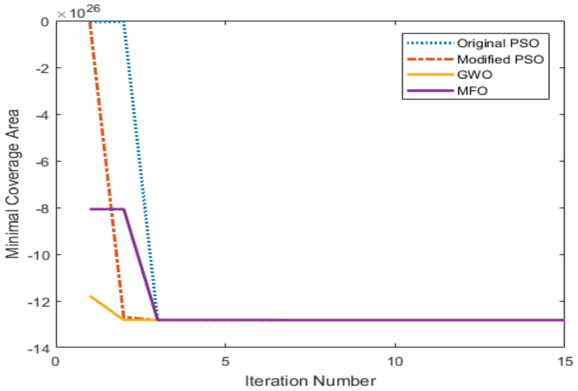


Fig. 28. Minimal Converges Area with F28.

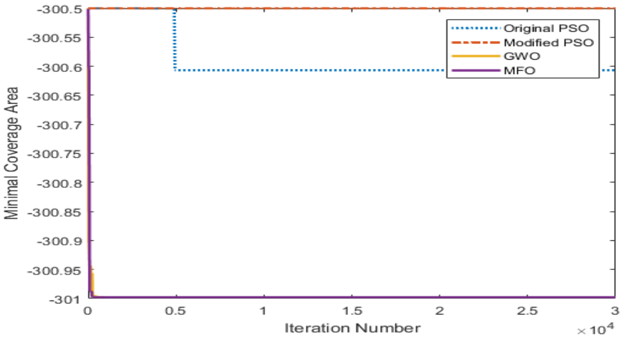


Fig. 29. Minimal Converges Area with F29.

B. Second Experiment Results and Discussion

In the second experiment, the Improved PSO was compared with PSO in mobile network environment. The comparison is based on minimal coverage area obtained with 100 iterations. Fig. 30 show the results of minimal coverage area vs. iterations.

The Improved PSO algorithm outperformed PSO algorithm. Because node positions update to get closer to the optimal node. Since all the nodes of the network get closer to the optimal location with each iteration, their coverage areas get smaller and smaller, and eventually reach zero and a jamming device can be conveniently placed there to disrupt the network. Improved PSO required less iterations compare to PSO to detect the optimal location of a jamming device. Fig. 31 show required number of iteration vs. number of experiments.

Table VI shows the statistical analysis results for Improved PSO and PSO. The obtained results show that Improved PSO outperformed PSO to optimal location for network coverage.

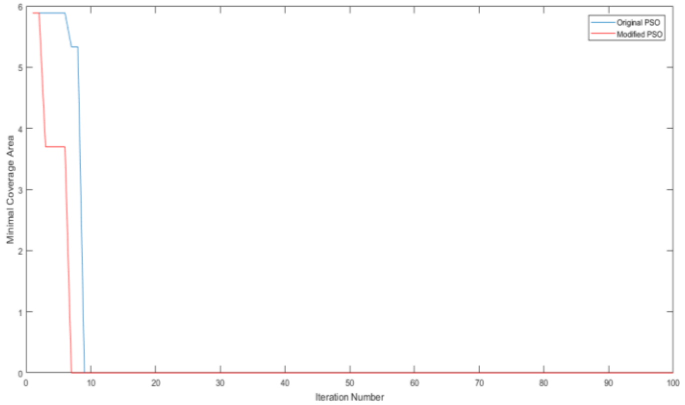


Fig. 30. Minimal Coverage Area Vs Iterations Number.

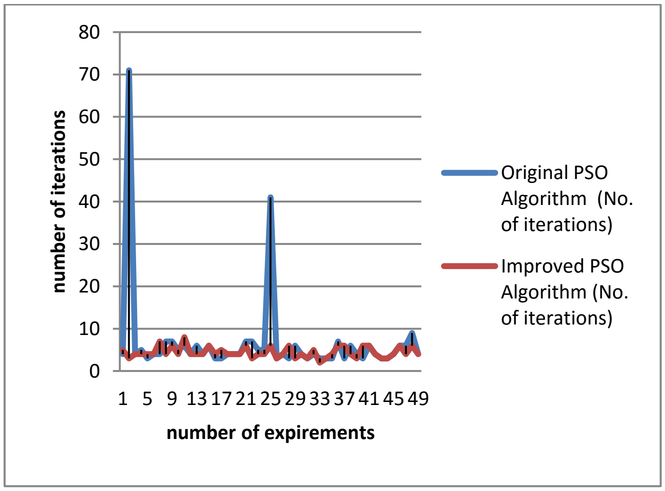


Fig. 31. Iteration Number vs. Run Number of Experiments.

TABLE VI. THE STATISTICAL ANALYSIS RESULTS FOR IMPROVED PSO AND PSO

PSO	Mean	Maximum	Minimum	Median	Mode
Original	6.64	71	3	4	4
Improved	6	80	3	4	4

V. CONCLUSIONS

The paper has proposed algorithm called Improved PSO. Improved PSO normalizing the entity positions and squaring the resulting fraction values to update the positions in faster way for every entity to reach the optimal location in the swarm. The Improved PSO as well was applied to a mobile network. The Improved PSO algorithm was evaluated with two experiments. In the First experiment, The Improved PSO was compared with PSO, GWO and MFO, obtained results shown the Improved PSO is the best algorithm among others to fine obtain the location for jamming attack. In Second experiment Improved PSO was compared with PSO in mobile network environment. The obtain results prove that Improved PSO is better than PSO for obtaining the location in mobile network where coverage area is minimal and hence central. The Improved PSO algorithm also improved the efficiency in detecting jamming attack and also improved source node determination for jamming attack.

REFERENCES

[1] Amrita Ghosal ,(2011), " A Jamming Defending Data-Forwarding Scheme For Delay Sensitive Applications In WSN", International Journal Of Computer Applications ,Volume 64– No.16.

[2] Barrera J. , Álvarez-Bajo O. , Flores J. And Coello C. ,(2016), "Limiting The Velocity In The Particle Swarm Optimization Algorithm", Computación Y Sistemas, Vol. 20, No. 4,Pp. 635–645.

[3] Nouaouria N.And Boukadoum M. ,(2011) , ''A Particle Swarm Optimization Approach To Mixed Attribute Data-Set Classification'', IEEE Symposium On Swarm Intelligence, Conference Paris, France.

[4] Muraleedharan R. Andosadciw L.A., "Jamming Attack Detection And Countermeasures In Wireless Sensor Network Using ANT System," Pg. 2.

[5] QuintanaC. , Rabadan J.And J. Rufo, F. Delgado And R. Perez-Jimenez, "Time-Hopping Spread-Spectrum System For Wireless Optical Communications," In IEEE Transactions On Consumer Electronics, Vol. 55, No. 3, Pp. 1083-1088, August 2009.

[6] Ramírez-Mireles F.,(2001), "Performance Of Ultrawideband SSMA Using Time Hopping And M-Ary PPM", IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 19, NO. 6,

[7] Houssaini M.A.E, Aaroud A., Hore A.E. And Ben-Othman J. ,(2016) ," Detection Of Jamming Attacks In Mobile Ad Hoc Networks Using Statistical Process Control", Procedia Computer Science, Vol. 83 PP. 26 – 33.

[8] Chaturvedi P. And Gupta K. ,(2013) ," Detection And Prevention Of Various Types Of Jamming Attacks In Wireless Networks" , International Journal Of Computer Networks And Wireless Communications ,Vol.3, No2.

[9] Thakur N. And Sankaralingam A. ,(2013) ," Introduction To Jamming Attacks And Prevention Techniques Using Honeypots In Wireless Networks" International Journal Of Computer Science And Information Technology & Security , Vol. 3, No.2, PP.202-207.

[10] Sari A. And Necat B. , (2012) ," SECURING MOBILE AD-HOC NETWORKS AGAINST JAMMING ATTACKS THROUGH UNIFIED SECURITY MECHANISM" International Journal Of Ad Hoc, Sensor & Ubiquitous Computing (IJASUC) ,Vol.3, No.3, PP.79-94.

[11] Xu W., Trappe W., Zhang Y.And Wood T. ,(2005) , " The Feasibility Of Launching And Detecting Jamming Attacks In Wireless Networks", ACM International Symposium On Mobile Ad Hoc Networking And Computing (Mobihoc), Vol. 2 , PP. 46-57.

[12] Balogun V. And A. Krings ,(2013) , " On The Impact Of Jamming Attacks On Cooperative Spectrum Sensing In Cognitive Radio Networks" , Proceedings Of The Eighth Annual Cyber Security And Information Intelligence Research Workshop , No. 31.

[13] Chowdary K.V. And Ali S.S. (2012) "Jamming Probability And Network Channel Access Probability In Wireless Sensor Networks", International Journal Of Computer Science & Software Technology, ISSN: 0974-3898, Vol 5, Number 1, PP. 49-51.

[14] Popli P. And Raj P. ,(2016)," Effect Of Jamming Attack In Mobile Ad Hoc Environment", International Journal Of Science, Engineering And Technology Research (IJSETR) Volume 5, Issue 5,PP.1521-1526.

[15] Pavani G. ,(2015)," Packet-Hiding Methods For Preventing Selective Jamming Attacks", International Journal Of Scientific & Engineering Research, Volume 6, Issue 10,PP.1011-1016.

[16] Pang, L., Chen, X., Shi, Y., Xue, Z., & Khatoun, R. (2017). Localization of multiple jamming attackers in vehicular ad hoc network. International Journal of Distributed Sensor Networks, 13(8), 1550147717725698..

[17] Suganthan, P. N., Hansen, N., Liang, J. J., Deb, K., Chen, Y. P., Auger, A., & Tiwari, S. (2005). Problem definitions and evaluation criteria for the CEC 2005 special session on real-parameter optimization. KanGAL report, 2005005(2005), 2005.

[18] Wang, L., & Wyglinski, A. M. (2011, August). A combined approach for distinguishing different types of jamming attacks against wireless networks. In Proceedings of 2011 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (pp. 809-814). IEEE.

[19] Adil, M.; Almaiah, M.A.; Omar Alsayed, A.; Almomani, O. An Anonymous Channel Categorization Scheme of Edge Nodes to Detect Jamming Attacks in Wireless Sensor Networks. Sensors 2020, 20, 2311.

[20] Adil, Muhammad, Rahim Khan, Mohammed Amin Almaiah, Mohammed Al-Zahrani, Muhammad Zakarya, Muhammad Saeed Amjad, and Rehan Ahmed. "MAC-AODV Based Mutual Authentication Scheme for Constraint Oriented Networks." IEEE Access 8 (2020): 44459-44469.

[21] Hudaib A., Al Hwaitat A.,(2018), " Movement Particle Swarm Optimization Algorithm" Modern Applied Science; Vol. 12, No. 1,pp.148-164

[22] Al Hwaitat A., Manaseer S.,(2018),Centralized Web Application Firewall Security System, Modern Applied Science; Vol. 12, No. 10; PP.164-170. https://doi.org/10.5539/mas.v12n10p164.

[23] Al Hwaitat A., Manaseer S. and Jabri R.,(2018) ,Distributed Detection and prevention of Web Threats in Heterogeneous Environment , ModernApplied Science; Vol. 12 ,No10 ,PP.13-22.https://doi.org/10.5539/mas.v12n10p13

[24] Al Hwaitat A., Manaseer S.,(2017),Validation and Integrity Mechanism for Web Application Security, International Journal of Engineering Research & Science , Vol. 3, No.11,PP.34-38. 29.

[25] Rababha O., Al Hwaitat A., Manasser S.,(2016) Web Threats Detection andPrevention Framework, communications and Network, Vol. 8, No.8, PP. 170178.

[26] Al Hwaitat A., Manaseer S., Al-sayyed R., m almaiah, o almomani ,(2020) , An Investigator Digital Forensics Frequencies Particle Swarm Optimization For Dectection And Classification Of Apt Attack In Fog Computing Environment (IDF-FPSO) ,Journal of Theoretical and Applied Information Technology, Vol.98 Issues 07.

APPENDIX 1. CEC 2005 TEST FUNCTIONS

Function Name	Function Equation	Dimensions (D)	Domain	Min
F1	$F_1(\mathbf{x}) = \sum_{i=1}^{D} z_i^{\,2}$	2	[-100,100]	0
F2	$F_2(\mathbf{x}) = \sum_{i=1}^{D} (\sum_{j=1}^{i} z_j)^2$	2	[-100,100]	0
F3	$F_3(\mathbf{x}) = \sum_{i=1}^{D} (10^6)^{\frac{i-1}{D-1}} z_i^2$	2	[-100,100]	0
F4	$F_4(\mathbf{x}) = (\sum_{i=1}^{D} (\sum_{j=1}^{i} z_j)^2) * (1 + 0.4 \lvert N(0,1) \rvert)$	2	[-100,100]	0
F5	$F_5(\mathbf{x}) = \max\{\lvert \mathbf{A}_i \mathbf{x} - \mathbf{B}_i \rvert\}$ **A** is a D*D matrix, a_{ij} are integer random numbers in the range [-*500, 500*], $\det(\mathbf{A}) \neq 0$, $\mathbf{A}_i$ is the i^{th} row of **A**. $\mathbf{B}_i = \mathbf{A}_i * \mathbf{o}$, **o** is a D*1 vector, o_i are random number in the range [-100,100]	2	[-100,100]	0
F6	$F_6(\mathbf{x}) = \sum_{i=1}^{D-1} (100(z_i^2 - z_{i+1})^2 + (z_i - 1)^2)$	2	[-100,100]	1
F7	$F_7(\mathbf{x}) = \sum_{i=1}^{D} \frac{z_i^{\,2}}{4000} - \prod_{i=1}^{D} \cos(\frac{z_i}{\sqrt{i}}) + 1$	2	[0,600]	1
F8	$F_8(\mathbf{x}) = -20\exp(-0.2\sqrt{\frac{1}{D}\sum_{i=1}^{D} z_i^2}) - \exp(\frac{1}{D}\sum_{i=1}^{D}\cos(2\pi z_i)) + 20 + e$	2	[-32,32]	-inf
F9	$F_9(\mathbf{x}) = \sum_{i=1}^{D} (z_i^{\,2} - 10\cos(2\pi z_i) + 10)$	2	[-5,5]	0
F10	$F_{10}(\mathbf{x}) = \sum_{i=1}^{D} (z_i^{\,2} - 10\cos(2\pi z_i) + 10)$	2	[-5,5]	0
F11	$F_{11}(\mathbf{x}) = \sum_{i=1}^{D} (\sum_{k=0}^{k\max} [a^k \cos(2\pi b^k (z_i + 0.5))]) - D \sum_{k=0}^{k\max} [a^k \cos(2\pi b^k \cdot 0.5)]$ a=0.5, b=3, $\mathrm{k_{max}}$=20, $\mathbf{z} = (\mathbf{x} - \mathbf{o}) * \mathbf{M}$, $\mathbf{x} = [x_1, x_2, ..., x_D]$	2	[-0.5,0.5]	-1
F12	$F_{12}(\mathbf{x}) = \sum_{i=1}^{D} (\mathbf{A}_i - \mathbf{B}_i(\boldsymbol{x}))^2$ $\mathbf{A}_i = \sum_{j=1}^{D} (a_{ij} \sin\alpha_j + b_{ij} \cos\alpha_j)$, $\mathbf{B}_i(x) = \sum_{j=1}^{D} (a_{ij} \sin x_j + b_{ij} \cos x_j)$, for $i = 1, ..., D$ D: dimensions **A**, **B** are two D*D matrix, a_{ij}, b_{ij} are integer random numbers in the range [-100,100], $\boldsymbol{\alpha} = [\alpha_1, \alpha_2, ..., \alpha_D]$, α_j are random numbers in the range $[-\pi, \pi]$.	2	[-π,π]	0
F13	F8: Griewank's Function: $F8(\boldsymbol{x}) = \sum_{i=1}^{D} \frac{x_i^{\,2}}{4000} - \prod_{i=1}^{D} \cos(\frac{x_i}{\sqrt{i}}) + 1$ F2: Rosenbrock's Function: $F2(\boldsymbol{x}) = \sum_{i=1}^{D-1} (100(x_i^2 - x_{i+1})^2 + (x_i - 1)^2)$ $F8F2(x_1, x_2, ..., x_D) = F8(F2(x_1, x_2)) + F8(F2(x_2, x_3)) + ... + F8(F2(x_{D-1}, x_D)) + F8(F2(x_D, x_1))$ Shift to $F_{13}(\mathbf{x}) = F8(F2(z_1, z_2)) + F8(F2(z_2, z_3)) + ... + F8(F2(z_{D-1}, z_D)) + F8(F2(z_D, z_1)) + f\_bias_{13}$	2	[-3,1]	1
F14	$F(x, y) = 0.5 + \frac{(\sin^2(\sqrt{x^2 + y^2}) - 0.5)}{(1 + 0.001(x^2 + y^2))^2}$ Expanded to $F_{14}(\mathbf{x}) = EF(z_1, z_2, ..., z_D) = F(z_1, z_2) + F(z_2, z_3) + ... + F(z_{D-1}, z_D) + F(z_D, z_1)$ $\mathbf{z} = (\mathbf{x} - \mathbf{o}) * \mathbf{M}$, $\mathbf{x} = [x_1, x_2, ..., x_D]$	2	[-100,100]	0