Path Optimization Using APSO

Deepak Goyal[1] and **Malay Ranjan Tripathy**[2]

Submitted in March, 2013; Accepted in August, 2013

Abstract - This paper addresses the malicious node detection and path optimization problem for wireless sensor networks. Malicious node detection in neighborhood is a needed because that node may cause incorrect decisions or energy depletion. In this paper APSO (combination of Artificial bee colony and particular swarm optimization) is used to choose an optimized path. Through this improved version we will overcome the disadvantage of local optimal which comes when we use PSO approach.

Index Terms - Green IT, Environmentally Sustainable, Environmental Intelligence (EI), Server Virtualization, Cloud Computing

1. INTRODUCTION

Wireless networks or sensor networks are composed of a large no. of dynamically located sensor nodes. The sensors collect the data and forward to the base station through defined communication path. Data is forwarded from source to sink node. If the information is sensitive, the nodes and communication path must be trust worthy. If any node in path is suspicious node need to calculate the alternative path.

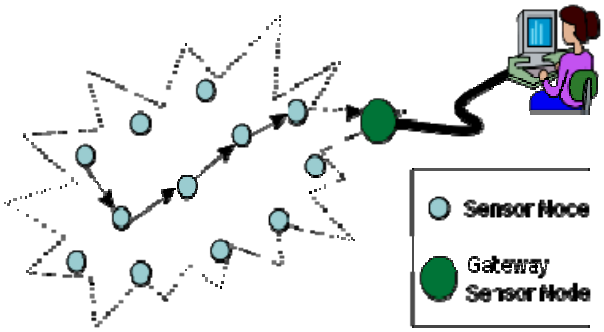

Figure 1: Wireless Sensor Network

Node may be suspicious due to internal reason like traffic load or external factors like temperature. There are many methods to calculate the trust of a node like Reputation-based, Event-based, Agent-based, etc.

As shown in figure 2 there are multiple paths from source to sink node but we have to choose optimized path. Now after detection of malicious node an alternate path is needed. There are so many strategies to find alternative path. Swarm Intelligence is the one of them. Swarm Intelligence itself has categories like Particle Swarm Optimization (PSO), Ant Colony Optimization (ACO), Artificial Bee Optimization (ABC), etc.

[1] *Jagannath University, Jaipur,* [2] *Amity University, Noida*
E-mail: deepakgoyal.vce@gmail.com and amity@gmail.com

Routing protocols may maintain single or multiple routes to a destination node. Single path protocols can find one or Multiple routes and so select the best path for data transport, discarding other ones and multipath routing refers to the protocols that find, maintain, and use those paths to transport sensed data [1].

Classical based Routing and Swarm Intelligence are one of the fields for path optimization. In [2] Authors compared many of these protocols. In this paper we would consider SI field.

2. RELATED WORK

2.1 PSO

Particle swarm optimization (PSO) is a popular multidimensional optimization technique. Ease of implementation, high quality of solutions, computational efficiency and speed of convergence are strengths of PSO. Advantages of PSO:

1) Ease of implementation on hardware or software.
2) Availability of guidelines for choosing its parameters.
3) Availability of variants for real, integer and binary domains.
4) Quick convergence [3].

In [4] paper, particle swarm algorithm was used to find the optimal positions of the sensors to determine the best coverage.

In [5] the modified form of PSO by the usage of an explicit consensus mechanism is used for optimization.

In [6] Authors consider the maximization of the coverage as an optimization criterion by implementing a centralized technique. Their technique is based on a modified PSO strategy they called their technique Particle Swarm Genetic Optimization (PSGO).

In [15] author considers Sensor Deployment Problem using Particle Swarm Optimization (PSO). This work has the ability to achieve optimal solution of coverage problem with minimum number of sensors in wireless sensor networks. This approach cultivates an innovative idea in employing the PSO algorithm with enhanced fidelity. The results show that the PSO approach is effective and robust for efficient coverage problem of sensor deployment and is considered to give almost the optimal solution in WSN.

In [16] the modified form of PSO by the usage of an explicit consensus mechanism is used for optimization. Author said that it is not useful to consider a global best position, because it implies a centralized scheme of control or, at least, the capacity of the nodes to communicate with every other node in the sensor field. In order to take into account the limited communication capabilities of sensors, we stated that the social term involves the position that enjoys the maximum consensus within each node's neighborhood, where a neighborhood is composed only of the sensors within its transmitting/receiving range.

In [17] author proposed a virtual force co evolutionary PSO for dynamic deployment of Nodes. Virtual force based dynamic

deployment involves iteratively moving a sensor based on virtual attractive or repulsive forces from other nodes, obstacles in the field and the areas that need higher coverage probability. Virtual force vectors depend on the distance between nodes and whatever attract or repulse them, and their relative directions. A sensor's new positions are computed in such a way that it moves in the direction of the virtual force by a step size proportional to its magnitude.

In [18] author used multi-base for optimal positioning of base station in a two tier WSN [17]. The two tier network consists of nodes that can communicate only with the application nodes they are assigned to. Application nodes possess long-range transmitters, high-speed processors, and abundant energy. The PSO Multi-Base method aims at determining positions of base stations so that the total of distances of application nodes to their nearest base stations is minimum..

In [19] Authors consider the maximization of the coverage as an optimization criterion by implementing a centralized technique. Their technique is based on a modified PSO strategy they called their technique Particle Swarm Genetic Optimization (PSGO).

2.1.1 Disadvantage of PSO

But there is a disadvantage of PSO which is local optimal because particle get flung away from the best location since global best value may be updated above a certain value so we need to keep track of how many iteration has passed since global best is updated.

2.2 ABC

It simulates the artificial bees to find out the best nectar source with swarm intelligence.

In [7] author applied the ABC algorithm to the dynamic deployment problem in WSNs with mobile sensors.

In [10] Author models the behavior of social insects, such as ants, birds or bees, for the purpose of search and in it problem solving has been the emerging area of swarm intelligence. Honey-bees is most closely studied social insects. Here, an artificial bee colony algorithm is developed to solve clustering problems which is inspired by the bees' forage behavior.

3. PROPOSED APPROACH

3.1 Detection of Malicious Node

If any node in the path is suspicious, that node is malicious and it is need to be detected Wireless sensor networks or sensor networks are composed of a large number of sensor nodes deployed densely in a closed proximity to collect data to a specific function. There are varieties of methods to calculate the trust of a successive node. The methods include the reputation-based trust management, event-based trust management, collaborative trust management, and agent-based trust management [8].

We would use Agent Based approach and Event Based approach.

3.2 Agent-Based Approach and Event-Based Approach:

Agent-based trust model for WSN can't distinguish different events which effect trust rating, and all the events have the same affects. Here, we propose a method in which different events considers to detect the nodes which can be faulty in different events.

In our trust framework, the trust rating is dependent on different events of the sensor nodes in WSN. It means that at different event, the node has different trust rating, which also means a sensor node has several trusting rating stored in its neighbor nodes.

Our trust framework runs at the agent node which has strong competence to compute, large storage and memory. The agent node uses Threshold value to monitor all kind of event happened in sensor nodes within its radio range and functions in a completely distributed manner. Threshold value is taken to be 4, if 4 or more packets comes to agent node then it would be considered as the high traffic and node can become faulty which would be protected by choosing another path as described in next section. Every agent node maintains trust table for nodes. In our framework, a node has several trusts rating value which would be stored at agent node. The number of trust rating in a sensor node depended on the number of events in sensor node. Here we store event trust of a node in a binary format. Here considers positive event and 0 shows negative event. This high traffic detection is needed because every node has some defined energy and node use this energy to send packets.

If heavy traffic attack to an agent node then energy of an agent node decreases suddenly and node may becomes faulty or maliciousness. In our work we set threshold such that we can stop traffic to an agent node before it becomes faulty.

In our trust framework first only one node tries to send packet to agent node as shown in figure 2. That event is trusted.

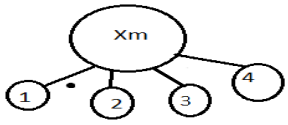

Figure 2: Event 1 where only one packet enters the agent node

Now let at Event 2, 4 packets tries to enter the agent node as in figure 4shown and we have set the threshold value 4 so now to save it from becoming dead node we would change the paths of all nodes which were used to go through it because now this node is at its peak value it will be dead as one more node will come to this node.

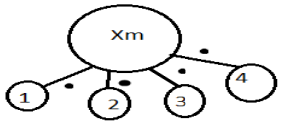

Figure 3: Event 2 where 4 Packets try to enter the agent node

In this paper after malicious node detection that node will inform its neighbors of its maliciousness and suggest another global best to calculate alternate path using modified version of PSO which

would be called APSO (Artificial Bee Particle Swarm Optimization). Addition of ABC will cover the limitation of PSO.

3.3 Particle Swarm Optimization

PSO algorithm works by having a population of particles.

Let *N* is the no. of particles in swarm, each having a position x_i in the search-space and a velocity v_i. Let p_i be the best position of the particle *i* and let g_b be the best position of the whole swarm.

Algorithm is:

For each particle $i = 1$ to N:

Initialize particle's position with uniformly distributed random vector: $x_i \sim U(b_{lo}, b_{up})$, b_{lo} and b_{up} are the lower and upper boundaries of the search-space. Initialize the particle's best position to its initial position: $p_i \leftarrow x_i$.

If ($f(p_i) < f(g_b)$) update the swarm's best position: $g_b \leftarrow p_i$

Initialize particle's velocity: $v_i \sim U(-|b_{u\ p} - b_{lo}|, |b_{up} - b_{lo}|)$ Until an end criterion is meet, repeat:

Step1.Count = 0

For every particle i = 1 to N:

For every dimension d = 1 to n:

Step2. Pick the random numbers: $r_p, r_g \sim U(0,1)$

Step3.Update particle's velocity: $v_{i,d} \leftarrow v_{i,d} + \varphi_p\, r_p\, (p_{i,d} - x_{i,d}) + \varphi_g\, r_g\, (g_{bd} - x_{i,d})$

Update particle's position: $x_i \leftarrow x_i + v_i$

Step4. If ($f(x_i) < f(p_i)$):

Update particle's best position: $p_i \leftarrow x_i$

Step5.If ($f(p_i) < f(g_b)$) update swarm's best position: $g_b \leftarrow p_i$

Step6.Now g_b holds the best solution. And call it Ta_best. Count = count+1.

The parameters φ_p, and φ_g are to be selected.

The function used here is sphere function whose global minimum value is 0 at (0, 0, …, 0). It is a unimodal function with non-separable variables.

$F(x) = \sum x^2$

3.3 APSO

The Process of APSO is as:

Step 1Initialization of Parameters: set number of individuals of the swarm; set maximum circle-index; set other constants needed.

Step 2 Initialization of the colony: firstly, generate a colony with specific number of individuals. Then as a bee colony, it is divided into two categories, each individual's fitness value; on the other hand, as a particle swarm, calculate the fitness value of each particle and take the best location as the global best location. We assume that the cyclic number is represented by iter, and iter +1.

Step 3 Perform Particle Swarm Optimization. The best location in the iteration will be called Ta _ best. There is a count variable which will be updated for each updation of the global best.

Step 4 If the global best is greater than 2 then run the Artificial Bee Colony Algorithm. After all the choices above have been made, the best solution is generated in this iteration which we called it GlobalMin.

Step 5 The minimum between the value of GlobalMin and the value Ta _ best is GlobalMins and is defined by the following equation:

Globalmins = globalmins, if globalmins <=Ta_best

globalmins = Ta_best, if Ta_best<=globalmins

And the GlobalMin and the Ta _ best will both be equal to the value GlobalMins, and will be substituted into next iteration iter=iter+1.

Step 6 If the number of circles is greater than the maximum of circle - index. If not, go to Step 2; if it is, end the process and save the value GlobalMins.

3.4 Artificial Bee Colony

It simulates the artificial bees to find out the best nectar source with swarm intelligence. Just like the artificial bee colony in reality, at this algorithm, all the artificial bees are mainly divided into two categories. One is called employed foragers. Their job is to gather honey from their corresponding nectar source, and to exchange information of their source with other bees. The specific employed foragers whose source is the best at the present will become the ones who lead others to their source. The other one is the unemployed foragers. They are the one who don't find out the suitable source by themselves. They can keep looking for the source or follow the lead foragers to gather honey. There are scouts, search the surrounding the nest and they try to find new food sources.The source is suitable or not is decided by the fitness value. The larger the fitness value, the better the sources is.

4. RESULTS

4.1 Parameters

Energy: As each node in the network is a sensor node, each node is defined with specific energy we have defined 6 Joules to each node. With each communication over the network some energy is lost. If the energy is less than minimum required energy or 0, the node will be dead itself. Here we keep Threshold 4 so as to prevent node from becoming dead.

Number of Packets: This property represents the number of successful packet coming to a cluster head for a specific communication.

Pbest: Particles own experience. It is location which particles remember where it was closer in the past means Particle knows its own best position.

Gbest: Whole swarm's best. The movements of the particles are guided by their own best known position in the search-space as well as the entire swarm's best known position. Particle choose minimum of the two.

Ta_best: Minimum of Pbest and Gbest.

Velocity: Initial velocity of packet is taken to be 5m/s. Particle changes its position by updating its location and velocity.

φ_p : 1/3

φ_g : 1/2

Gloabalminimum: Employed foregoers, they are keeping searching the new sources around them and determine which one

is turned to according to the minimum fitness value of each source which we called it GlobalMin.
Threshold: We have taken 4 as its value at the time of detecting malicious node. When this value comes node is said to be malicious.
Count: We have taken its value to be 2. It is used to check how many times global best is updated. When this value exceeds colony is updated from Particle Swarm Optimization to Artificial Bee Colony so that particle does not trap in local optimal problem.
Count1: Shows the no. of times a packet can go to the sink nodes using PSO in the same time as compared to APSO.
Count2: Shows the no. of times a packet can go to the sink nodes using APSO in the same time as compared to PSO.

4.2 Results and Discussion

A node wants to send a packet to its sink node. For it node send packet to its agent node which would send further agent of sink node (figure 6). This is called event 1 so it is a Positive event.

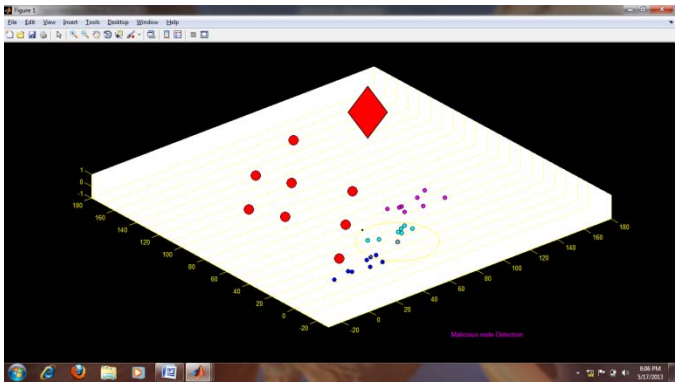

Figure 4

As discussed in earlier section that this trust framework runs at the agent node which has strong competence to compute, large storage and memory. The agent node uses Threshold value to monitor all kind of event happened in sensor nodes within its radio range and functions in a completely distributed manner. Threshold value is taken to be 4, if 4 or more packets comes to agent node then it would be considered as the high traffic and node can become faulty which would be protected by choosing another path as described in next section. Every agent node maintains trust table for nodes. So in this paper we use high traffic load as a malicious measure. If packets greater than threshold value which is 4 try to enter the agent node to send their packets to sink node. So it cause high traffic load on agent node (figure 7). This is event 2 and is negative event.

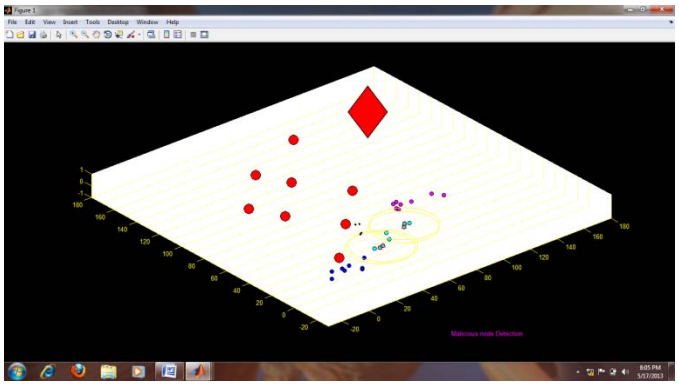

Figure 5

Now Event – Based approach is applied to the agent node and node becomes yellow to show high traffic load. As energy gets lost with each communication agent node would not be able to tackle all packets at a time because this may cause fault to the agent node and so if value of threshold reaches agent node stop working.

The second agent node is detected as bad nodes (shown in yellow). This bad node does not allow pass packets to the next nodes. It informs its neghibour nodes to choose another path to sink node. And by applying APSO we calculated new path. So, aafter the bad node is detected, packets changed their path to reach the destination based on APSO. Firstly our algorithm use concept of PSO (figure 8).

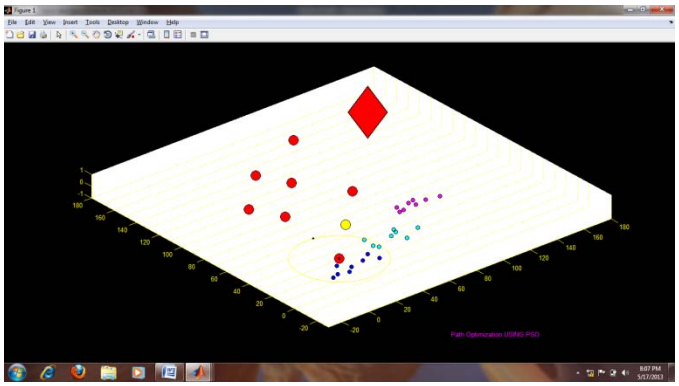

Figure 6

As we have used count limit is 2 so after it becomes two it uses the concept of Artificial Bee as there is possibilities of coming more new nodes which may lead to better path. As in Artificial bee scout helps in finding new source. Here both PSO and ABC find their best and these are compared and we choose the best one for next location. And now local optimum (discussed in earlier section) of PSO is removed (figure 9). New nodes are represented by cyan colour.

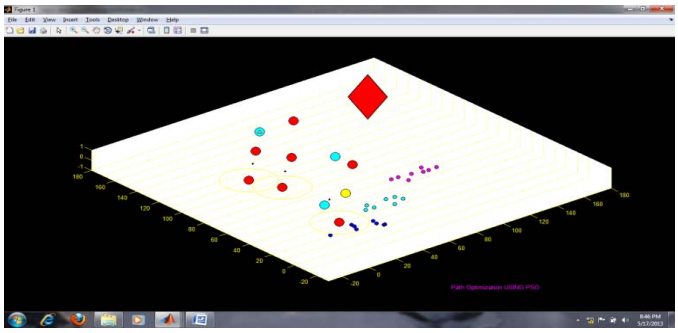

Figure 7

Now Artificial bee found new better route and now it can be used (figure 10).

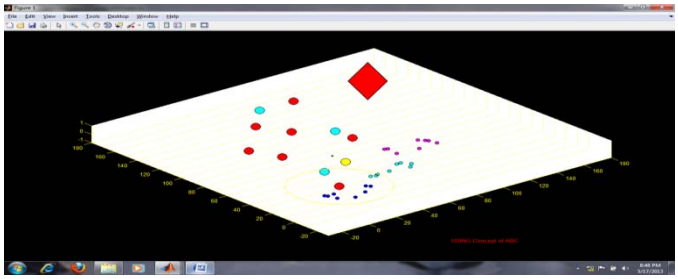

Figure 8

Now we calculate the no. of times a packet can go to the sink nodes using APSO in the same time as compared to PSO. We would count it through two variables count1 (for PSO), count2 (for APSO). This is shown in table1 in next part below.

4.3 Graph of Malicious node Detection

At event 1 as discussed in results it is positive event and we have chosen 1 as a trust value for positive event.

At event 2 as discussed in result it is negative event and it is not trusted one and we will show it as 0 value for trust value of node which will force us to change the direction to sink node and we have chosen APSO algorithm to do that. This is shown in figure 11.

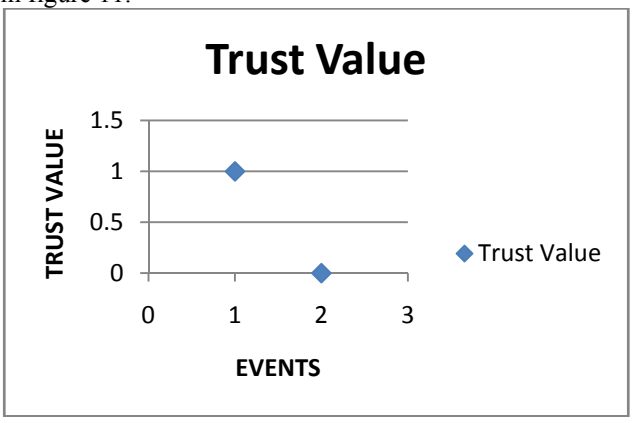

Figure 9: Trust Rating

4.3.1 Comparison of PSO and APSO

As we have discussed before there is a limitation of PSO that it can trap in local optimum. If after trapping in local optimum of PSO we use only PSO the following graph is made. Figure 12 shows the distance travelled by packets.

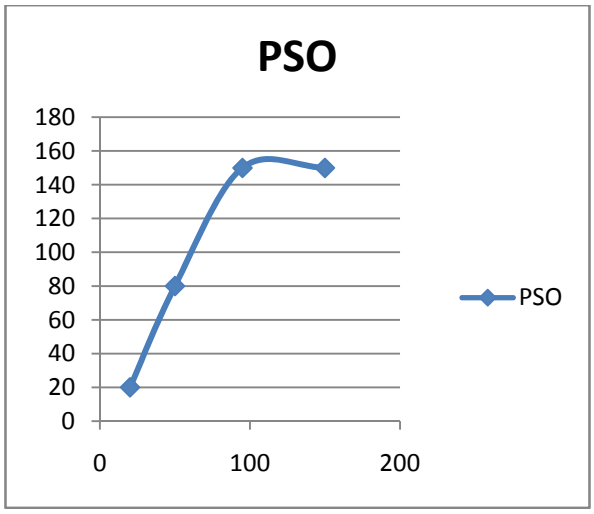

Figure 10: Path chosen by PSO

But if we use our APSO we found that a new better path has come and this makes packet to go through a best shortest path as shown in following graph. Figure 13 shows distance travelled by packets. So now we can say that our proposed Algorithm (APSO) is better than PSO.

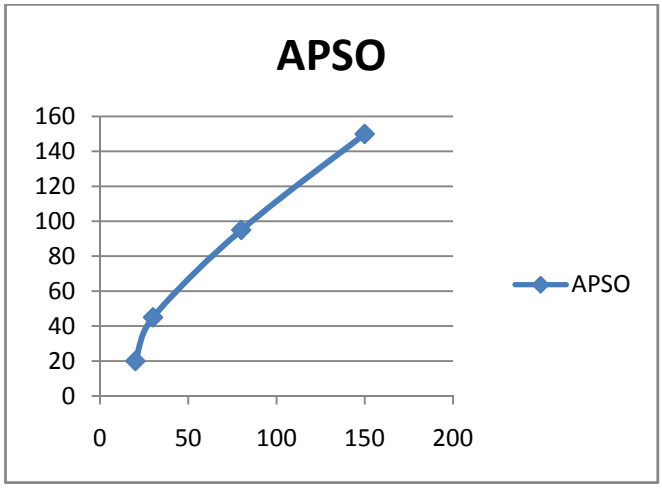

Figure 11: Path chosen by APSO

Chosen Strategy	Packet Delay	Value of count1, count2
PSO	More (because packets are going through long path and APSO can	Count1=1

	send two times in the same time of PSO)	
APSO	Less	Count2=2

Table 1: Comparison of packets delay in PSO and APSO

After implementing APSO packets transmitted (figure 14) over the network is increased as compared to PSO (figure 15) in minimum time because packets are transmitted through the shortest path. Packet delay is shown in table 1. This is counted by count1 (for PSO) and count2 (for APSO) variables in our proposed work.

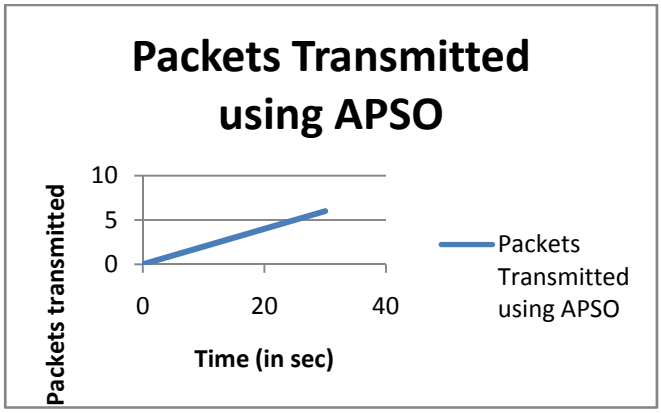

Figure 12

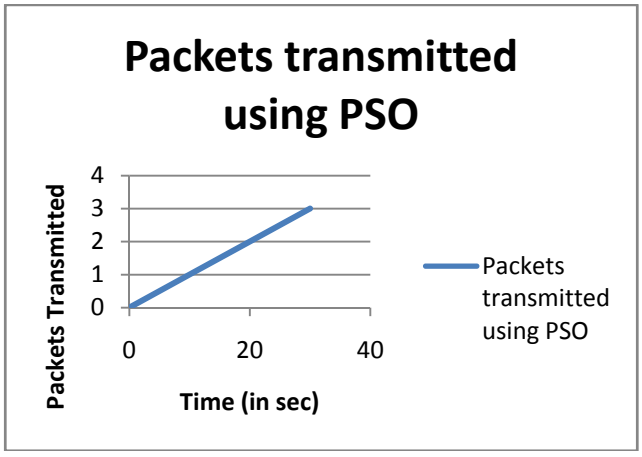

Figure 13

5. CONCLUSION

In this paper we consider high traffic load as a measure of malicious node. It is nature of these networks that higher traffic load is observed in some events.Here we use Agent-based approach with different events for detection of node before it becomes a faulty node and that detected node informs its entire neighbour about its maliciousness to choose another path and also we use an combine approach of Artificial bee colony and PSO called APSO to choose on optimized path. After detection of malicious node due to high traffic load we calculated alternate path using modified PSO (APSO). As a result APSO can send two times more packets in the same times of PSO ,we use our APSO we found that a new better path has come and this makes packet to go through a best shortest path and thus it overcomes the disadvantage of PSO which is used to get trap in the local optimal.

REFERENCES

[1] Gianni A. Di Caro, Muddassar Farooq and Muhammad Saleem,, "Swarm Intelligence Based Routing protocol for Wireless Sensor Networks: Survey and Future Directions", ELSEVIER, Information Sciences, Volume 181, Issue 20, 15 October 2011, pp. 4597–4624.

[2] Adamu MurtalaZungeru, KahPhooiSeng and Li-MinnAng, "Classical and swarm intelligence based routing protocols for wireless sensor networks: A survey and comparison", Journal of Network and Computer Applications 35, 2012, 1508–1536.

[3] Ganesh Kumar Venayagamoorthy and Raghavendra V. Kulkarni, "Particle Swarm Optimization in Wireless Sensor Networks: A Brief Survey",IEEE Transactionson Systems, MAN, and CYBERNETICS, March 2010.

[4] Babu Rao Thella, Nikitha Kukunuru, and Rajya Lakshmi Davuluri, "Sensor Deployment Using Particle Swarm Optimization", Nikitha et. al. / International Journal of Engineering Science and Technology, vol. 2(10), 2010.

[5] Enrico Natalizio, Francesca Guerriero, Valeria Loscrí, "Particle Swarm Optimization Schemes Based on Consensus for Wireless Sensor Networks", MSWiM, 2012.

[6] J. Li, K. Li, and W. Zhu, "Improving sensing coverage of wireless sensor networks by employing mobile robots", in Proc. Int. Conf. Robot. Biomimetics, pp. 899-903, 2007.

[7] Beyza Gorkemli, Celal Ozturk and Dervis Karaboga, "Artificial Bee Colony Algorithm for Dynamic Deployment of Wireless Sensor Networks", Turk J Elec Eng & Comp Sci, Vol.20, No.2, 2012.

[8] Yenumula B. Reddy, "Trust-Based Approach in Wireless Sensor Networks Using An Agent to Each Cluster", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol.1, No.1, February 2012.

[9] Alex Doboli, ,Constantin Volosencu, Daniel-Ioan Curiac, Octavian Dranga and Tomasz Bednarz, "Neural Network Based Approach for Malicious Node Detection in Wireless Sensor Networks", Proceedings of the 2007 WSEAS Int. Conference on Circuits, Systems, Signal and Telecommunications, Gold Coast, Australia, January 17-19, 2007.

[10] Changsheng Zhang, Dantong Ouyang, Jiaxu Ning, "An artificial bee colony approach for clustering", ELSEVIER, Expert Systems with Applications 37, 2010, 4761–4767.