SWARM INTELLIGENCE TECHNIQUE FOR SINKHOLE ATTACK DETECTION IN WIRELESS SENSOR NETWORK USING ABC ALGORTHM

Dharshini Y N[1], Chinnaswamy C N[2]

[1]*PG student, Department of ISE,NIE college,Mysuru,Karnataka,India*
[2]*Associate Professor, Department of ISE,NIE college,Mysuru,Karnataka,India*

Abstract

Data sensing, processing and communicating is an inevitable requirement in monitoring environment or physical conditions. The rudiment of WSN satisfies this stipulation of monitoring systems in different areas and is widely favored in numerous sensitive systems. Security concerns is a fervently discussed topic by the research community as the probability of vulnerable attacks is more in WSN. This research work focuses on enhancing the security of WSN by efficiently detecting sinkhole attack. Sinkhole attack is more intense as it results in bringing in other varieties of intrusions. Detection schemes depend on computational intelligence and Swarm Optimization is a commonly preferred approach. In our work, existing intrusion detection algorithm using Enhanced Particle Swarm Optimization (EPSO) was compared with a proposed Artificial Bee Colony (ABC) technique. The proposed ABC approach yielded improvement in terms of Detection rate, False Alarm rate, Packet delivery ration, Message drop and Average delay. These results promise a better intrusion detection scheme than the existing EPSO technique.

Keywords: *EPSO,ABC,Sinkhole,WSN's*

1. INTRODUCTION

Wireless Sensor Networks (WSN) is one of the most extensively experimenting and widely adopting technology in contemporary scientific world, as information gathering and processing in real time has turned an inevitable desideratum. In such a scenario, the significance of studying the security and possible threats related to WSN seeks great demand. Besides, deployment of WSN applications in remote areas makes it more pregnable. Referring to literature and current studies, there are copious resources pointing to various types of vulnerable attacks perturbing WSN and preponderance of them highlights security problems as the foremost concern.

Selective Forwarding Attack, Sinkhole Attack, Sybil Attack, Wormhole Attack, Hello Flood Attack, Black hole Attack and Node Replication attack are some of the dogged WSN attacks that transforms the system to an impuissant state[1].We consider sinkhole attack particularly for this study as it is an especially dangerous attack that prohibits the base station to gain entire and correct sensing data, consequently making a severe threat to the higher layer application. In a sinkhole, the adversary's goal is to lure nearly all the traffic from a particular area through a compromised node, creating a metaphorical sinkhole with the adversary at the center.

A compromised sensor node attempts to impact the information to it from any neighboring node. Thus, sensor node eavesdrops on each information is being communicated with its neighboring sensor nodes. Sinkhole attack works by making a compromised node look especially attractive to surrounding nodes with respect to the routing algorithm. For example, an adversary could spoof or reply an advertisement for an extremely high quality rout to the base station[2]. Moreover, once sinkhole attack infiltrate into a network, it is capable of effectuating Selective Forwarding Attack, Wormhole Attack,

Flooding Attack, Sybil Attack and Black hole Attack[3].

Swarm Intelligence (SI) is one of the effective methods that can be applied for sinkhole attack detection. It uses the collective behavior of decentralized, self-organized systems, natural or artificial. Advantages of SI are Flexibility, Robustness, Scalability and it is decentralized and self-organized. There are two popular swarm inspired methods namely, Ant Colony Optimization (ACO) and Particle Swarm Optimization (PSO).

It is observed that, so far only Ant Colony Optimization algorithm,Particle Swarm Optimization are applied for sinkhole detection. Further, not all swarm intelligence methods are explored for sinkhole detection. Out of the two, PSO method is found to be efficient in sinkhole attack detection. Hence, the existing PSO is enhanced using hash table and EPSO is considered as efficient compared to ACO and PSO.

2. PROPOSED SOLUTION

This research work proposes a heuristic experimental approach to evaluate the computational efficiency in intrusion detection by employing ABC, one of the popular swarm intelligence method to replace the existing EPSO technique. Sinkhole detection is one of the imperative requirements of security platform for ensure a reliable working environment of WSN. The work compares EPSO and ABC approaches in similar WSN environment using NS2 simulator. An attacker was introduced and transformed to sinkhole by attracting traffic. The situation was experimented and compared using ABC and EPSO methods. Realistic simulation environment is a promised output of NS2 simulator and the results were monitored to analyze the efficiency. Performance evaluation and validation pointed out ABC as a more efficient scheme for implementing in intrusion detection schemes.

3. METHODOLOGY OVERVIEW

The subject was studied through a specific research plan and was simulated using Network Simulator 2 (NS2) software tool. Wireless Sensor Networks were simulated in NS2 environment by creating a network model. A threat model was created by injecting sinkhole attack followed by data collection. At the outset, EPSO was applied for sinkhole detection which was the existing method taken for reference. This was followed by the proposed method of detection using ABC. Eventually the experimental results were compared to judge the best algorithm.

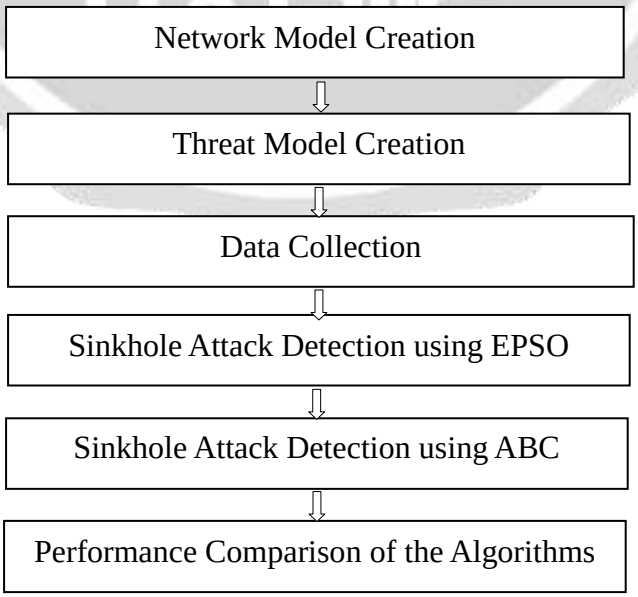


Figure 3.1 : Methodology Overview

- **Creating Network Model and Threat Model**

WSN network was modelled using NS2 software tool. NS2 supports simulations of TCP and UDP, MAC layer protocols, routing and multi-cast protocols in WSN. WSN network scenario was simulated using 50 nodes and was followed by threat network model was generated by injecting sinkhole attack.

- **Data Collection**

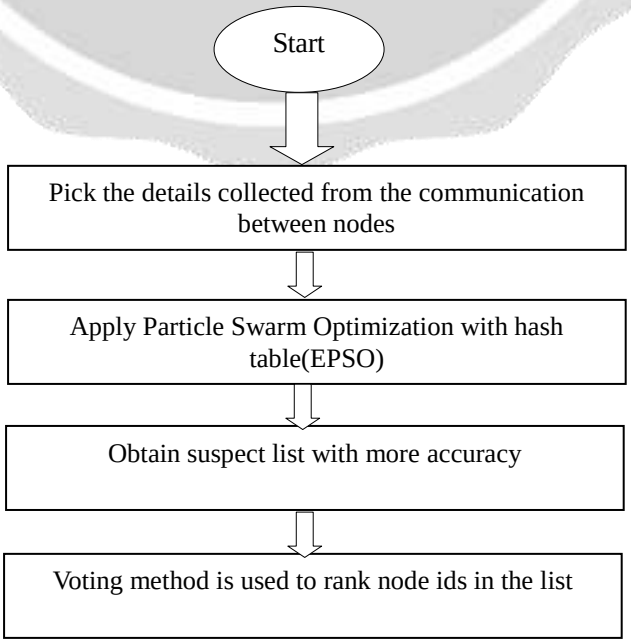
Followed by network creation, the sensor nodes started communicating each other detecting the network topology. Source node id, Destination node id, Packets sent, Packet received and size of packets are the data collected from the communication between nodes.

- **Detecting Sinkhole Attacks using Enhanced Particle Swarm Optimization**

PSO mimics the practices of feathered creature flocking.In PSO, each single arrangement is a "winged animal" in the hunt space. We call it "molecule". All of particles have wellness esteems which are assessed by the wellness capacity to be enhanced, and have speeds which coordinate the flying of the particles.The particles fly through the issue space by taking after the present ideal particles.PSO is introduced with a gathering of irregular particles (arrangements) and after that scans for optima by refreshing eras.

In each emphasis, every molecule is refreshed by taking after two "best" qualities. The first is the best arrangement (wellness) it has accomplished up until this point. (The wellness esteem is additionally put away.) This esteem is called pbest.Another "best" esteem that is followed by the molecule swarm streamlining agent is the best esteem, acquired so far by any molecule in the populace. This best esteem is a worldwide best and called gbest.When a molecule removes a portion of the populace as its topological neighbors, the best esteem is a nearby best and is called lbest.

Subsequent to finding the two best esteems, the molecule refreshes its speed and positions.In EPSO, Hash table is additionally utilized as a part of voting technique. Hashing has been beforehand proposed to record the arrangements experienced amid late emphasess. All arrangements explored amid a pursuit are put away in a rundown, called arrangement list. A hash capacity is utilized as a pointer to rapidly get to the arrangements put away in arrangement list. A moment list, called impact rundown is utilized to store arrangements with a hash crash. This system works adequately in recognizing assaults.



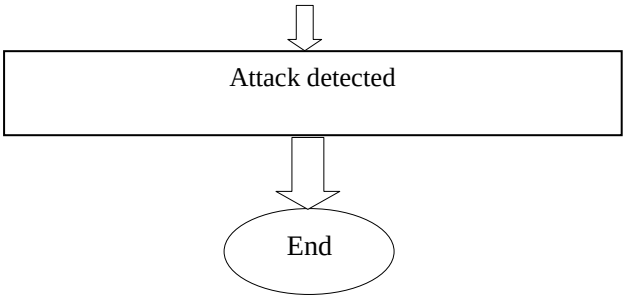
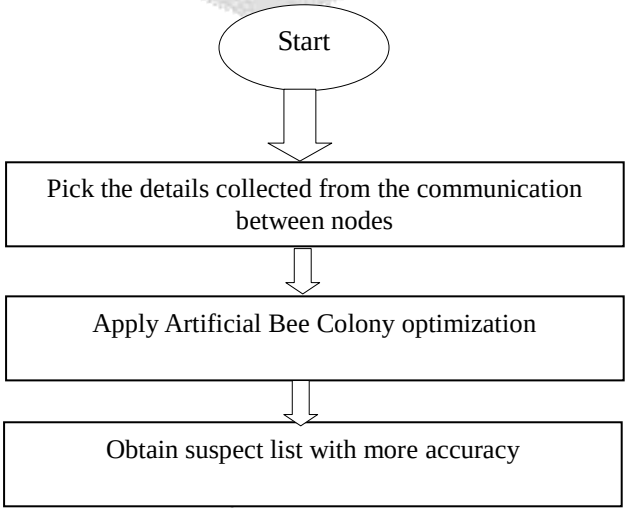


Figure 3.2 :Flowchart of EPSO

- **Detecting Sinkhole Attacks using Artificial Bee Colony Optimization**

The ABC algorithm is a swarm based, meta-heuristic algorithm in light of the searching conduct of bumble bee colonies.The ABC comprises of three gatherings of simulated honey bees: employed foragers,onlookers and scouts. The employed honey bees contain the principal half of the state though the second half comprises of the onlookers.The employed honey bees are connected to specific sustenance sources. As it were, the quantity of employed honey bees is equivalent to the quantity of nourishment hot-spots for the hive. The onlookers watch the move of the employed honey bees inside the hive, to choose a sustenance source, though scouts look haphazardly for new nourishment sources.

The pursuit cycle of ABC comprises of three guidelines: (i) sending the employed honey bees to a nourishment source and assessing the nectar quality; (ii) onlookers picking the sustenance sources in the wake of acquiring data from employed honey bees and computing the nectar quality; (iii) deciding the scout honey bees and sending them onto conceivable sustenance sources. The places of the nourishment sources are haphazardly chosen by the honey bees at the in-statement arrange and their nectar qualities are measured. The employed honey bees then offer the nectar data of the sources with the honey bees holding up at the move zone inside the hive. In the wake of sharing this data, each employed honey bee comes back to the sustenance source gone to amid the past cycle, since the position of the nourishment source had been retained and afterward chooses another nourishment source utilizing its visual data in the area of the present one. At the last stage, a passerby uses the data acquired from the employed honey bees at the move zone to choose a sustenance source. The likelihood for the sustenance sources to be chosen increments with increment in its nectar quality. Along these lines, the employed honey bee with data of a sustenance source with the most noteworthy nectar quality enlists the onlookers to that source. It in this way picks another nourishment source in the area of the one right now in her memory in view of visual data (i.e. examination of nourishment source positions). Another sustenance source is arbitrarily created by a scout honey bee to supplant the one relinquished by the onlookers honey bees.



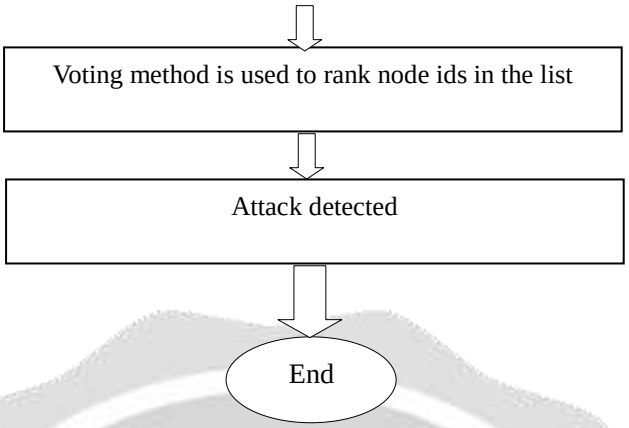
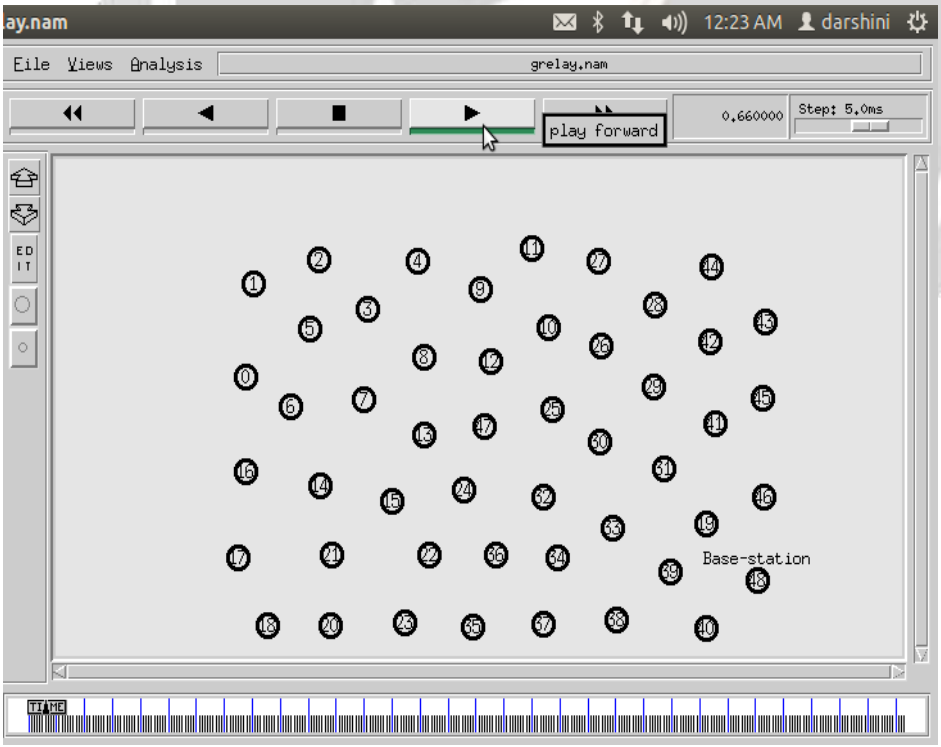


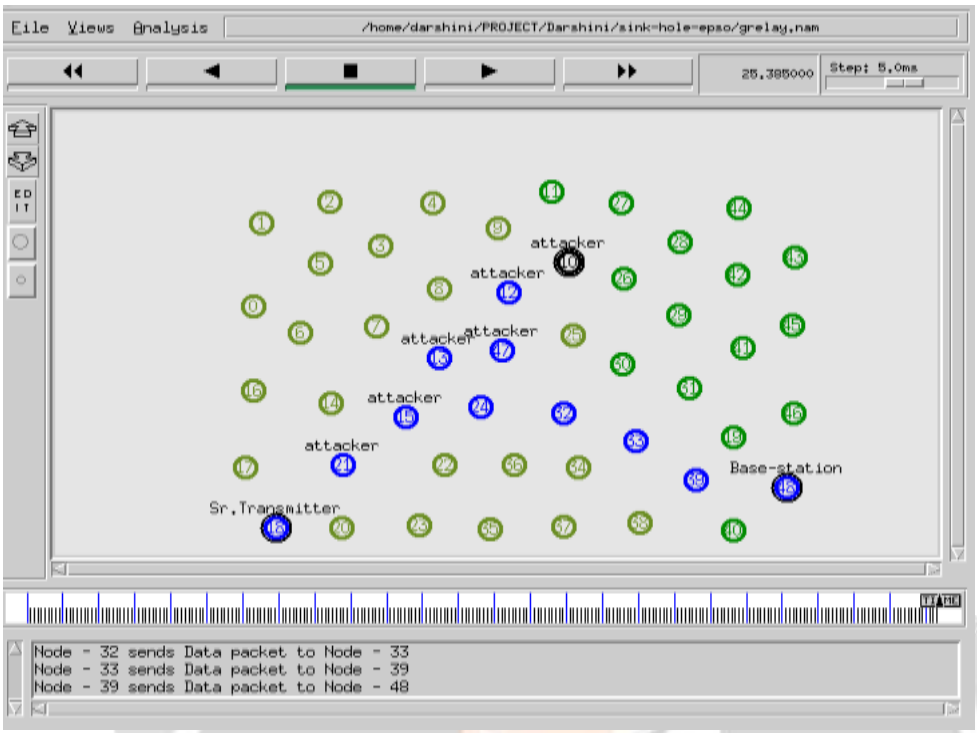
Figure 3.3:Flowchart of ABC

4. RESULTS

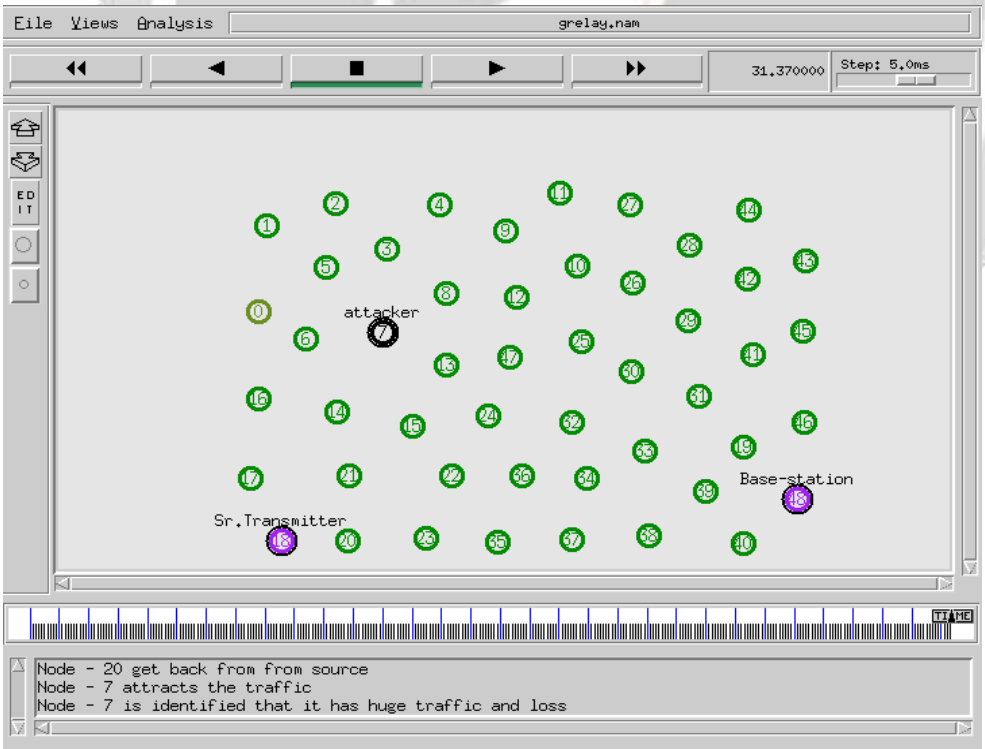
The subject was studied through a specific research plan and was simulated using Network Simulator 2 (NS2) software tool.



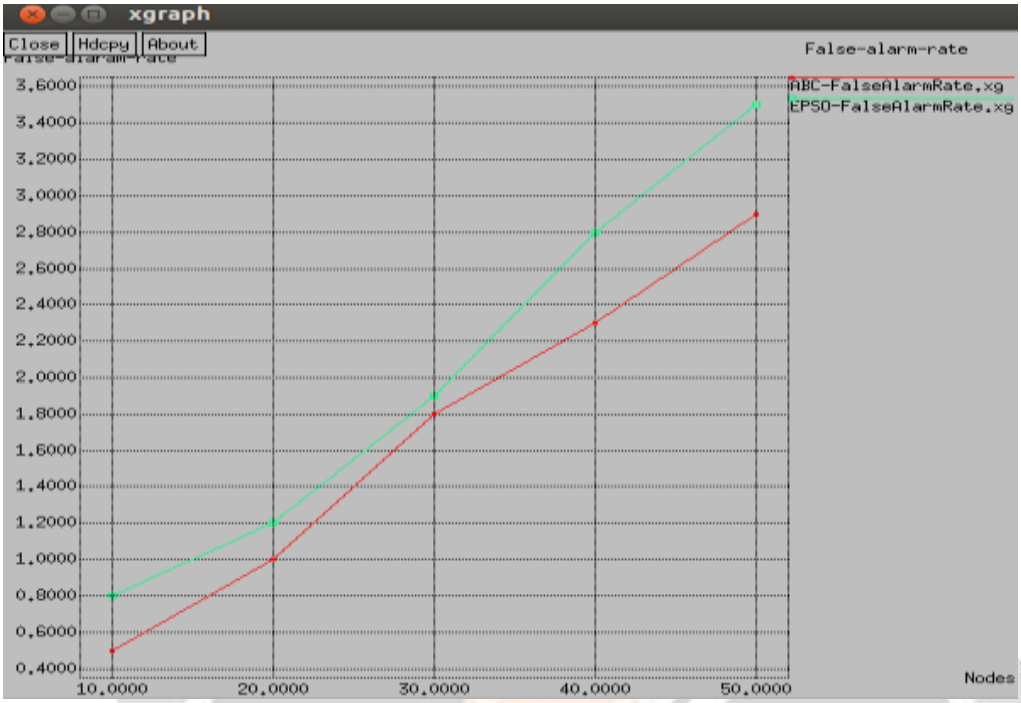
Network model of 50 Nodes



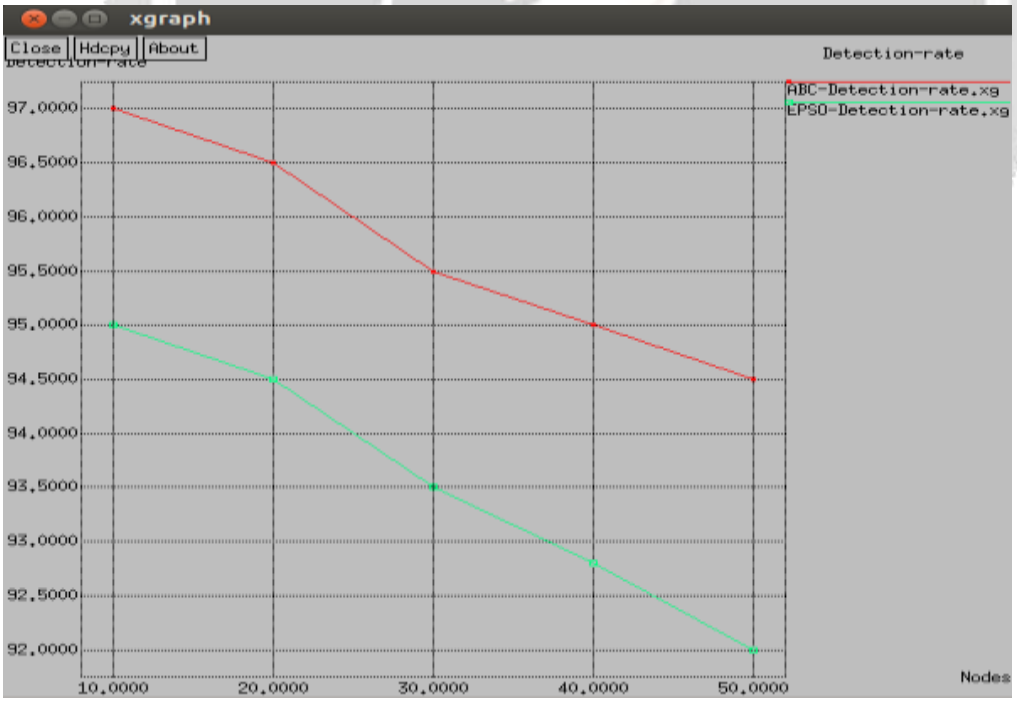
Threat Model using Existing EPSO with node 18 as source and 48 as base station



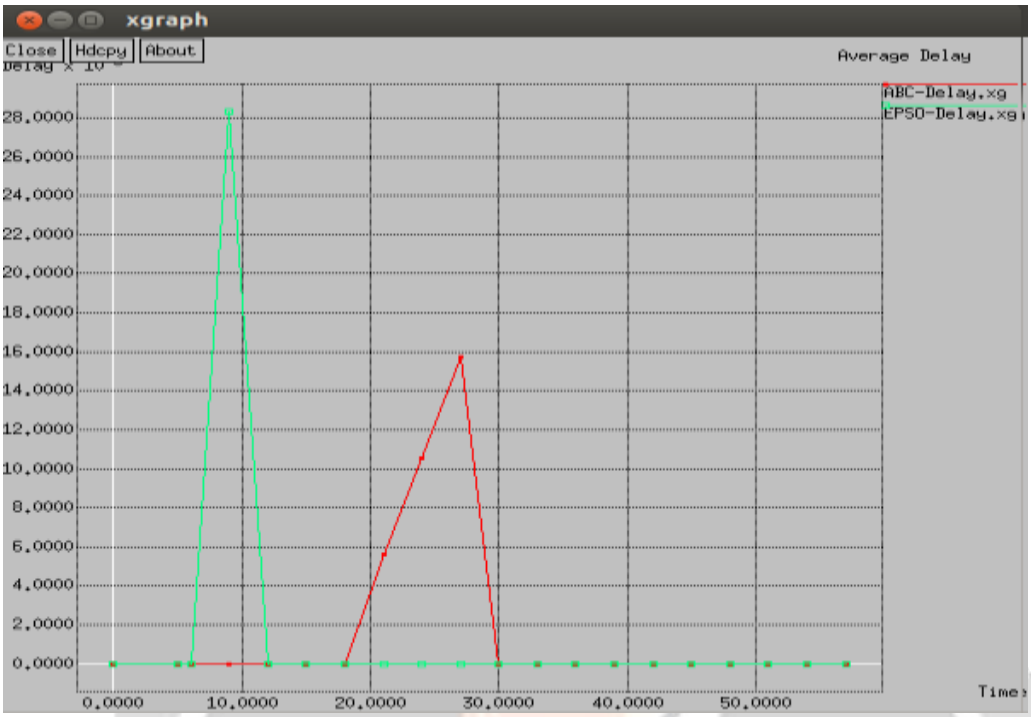
Threat Model using Proposed ABC with node 18 as source and 48 as base station



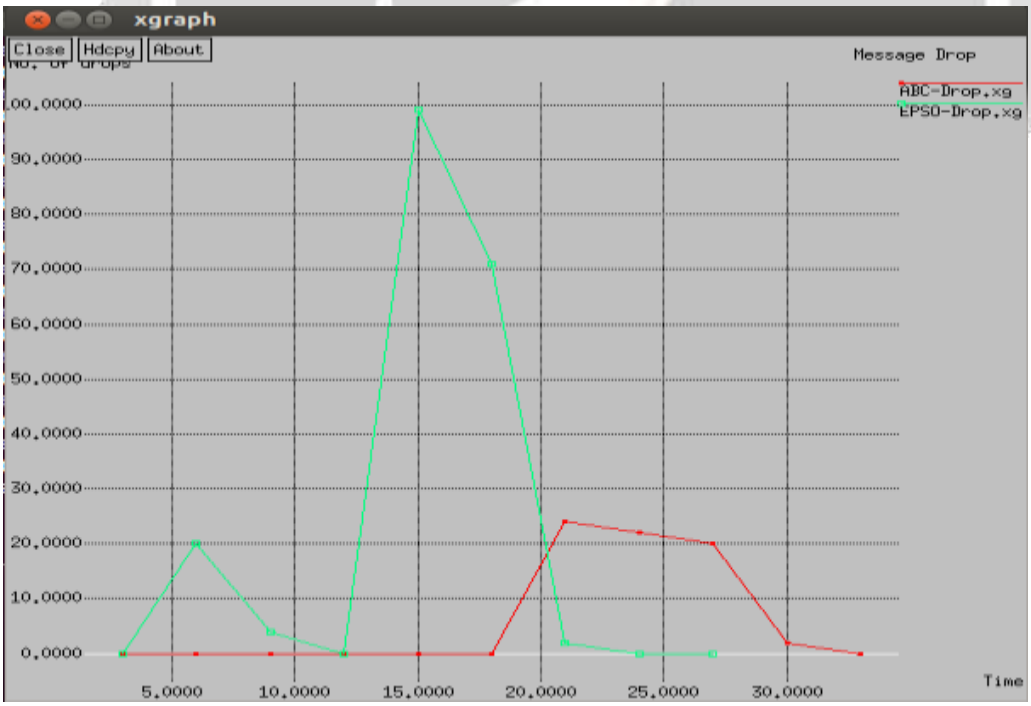
False Alarm Rate



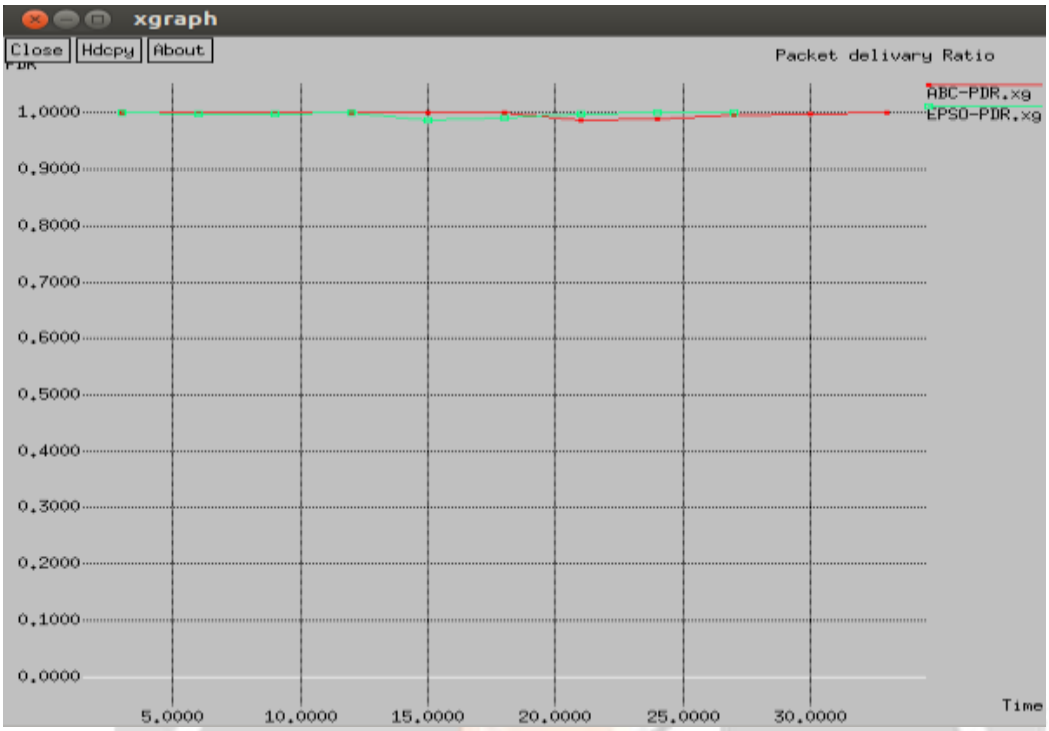
Detection Rate



Average Delay



Message Drop



Packet Delivery Ratio

5. CONCLUSION AND FUTURE ENHANCEMENT

WSN has become ubiquitous due to the increased demand of automation and wide scale deployment of remote monitoring systems. Security concern is a main caveat and its imperative to ensure impeccable working of these systems. The project opens a new proposal with security and intrusion detection in WSN by experimenting swarm intelligence. The results delineate amelioration of efficiency in currently existing intrusion discernment methods. We followed a heuristic approach by employing EPSO and ABC algorithms in same WSN environment for sinkhole detection using NS2 simulator. The results were intriguing and the proposed ABC algorithm was giving improved outputs compared to existing EPSO approach. We found that ABC exhibited **75%** decrease in message drop rates , **2%** increase in detection rate, **53%** decrease in average delay ,**18%** decrease in false alarm rate and slight improvement in packet delivery ratio compared to EPSO.

Our work is a new thread to the research enthusiasts to get motivated and explore more applications in swarm intelligence and exercise it in the security and computation fields of WSN.The improvement of convergence speed in ABC by changing the search pattern of onlooker and employed bees is considered as future work.

6. BIBILOGRAPHY

[1.] H Jadidoleslamy, "A Comprehensive Comparison of Attacks in Wireless Sensor Networks", International Journal of Computer Communications and Networks, Vol. 4, Issue 1, (2014).

[2.] Karlof, C. and Wagner, D., "Secure routing in wireless sensor networks: Attacks and countermeasures", Elsevier's Ad Hoc Network Journal, Special Issue on Sensor Network Applications and Protocols, September 2003, pp. 293-315.

[3.] L Rajakumaran , R Thamarai Selvi, "Detection Techniques of Sinkhole Attack in WSNs: A Survey", International Journal of Engineering Science Invention, Volume 3, Issue 6, (2014), pp.12-14.

[4.] J. Kennedy and R. Eberhart, "Particle swarm optimization," in Proceedings of the IEEE International Conference on Neural Networks, pp. 1942–1948, December 1995.

[5.] D. Karaboga and B. Akay, "A comparative study of artificial Bee colony algorithm," Applied Mathematics and Computation, vol. 214, no. 1, pp. 108–132, 2009.

[6.] G. Zhu and S. Kwong, "Gbest-guided artificial bee colony algorithm for numerical function optimization," Applied Mathematics and Computation, vol. 217, no. 7, pp. 3166–3173, 2010.