International Journal of Security and Its Applications
Vol. 10, No. 3 (2016), pp.41-54
http://dx.doi.org/10.14257/ijsia.2016.10.3.05

Detecting Sinkhole Attack in Wireless Sensor Network using Enhanced Particle Swarm Optimization Technique

[1]G. Keerthana, [2] G. Padmavathi

[1]Research Scholar, [2]Professor and Head
[1,2]Department of Computer Science,
[1,2]Avinashilingam Institute for Home Science and Higher Education for Women,
[1,2]Coimbatore, India
[1]keerthana2492@gmail.com, [2]ganapathi.padmavathi@gmail.com

Abstract

Wireless Sensor Network (WSN) is a collection of tiny sensor nodes capable of sensing and processing the data. These sensors are used to collect the information from the environment and pass it on to the base station. A WSN is more vulnerable to various attacks. Among the different types of attacks, sinkhole attack is more vulnerable because it leads to a variety of attacks further in the network. Intrusion detection techniques are applied to handle sinkhole attacks. One of effective approach of intrusion detection mechanism is using Swarm Intelligence techniques (SI). Particle Swarm Optimization is one of the important swarm intelligence techniques. This research work enhances the existing Particle Swarm Optimization technique and the proposed technique is tested in a simulated environment for performance. It is observed that the proposed Enhanced Particle Swarm Optimization (EPSO) technique performs better in terms of Detection rate, False Alarm rate, Packet delivery ration, Message drop and Average delay when compared to the existing swarm intelligence techniques namely, Ant Colony Optimization and Particle Swarm Optimization.

Keywords*: Wireless Sensor Network, Sinkhole Attack, Swarm Intelligence, Ant Colony Optimization, Particle Swarm Optimization*

1. Introduction

Wireless Sensor Network (WSN) is one of the popular network types applied in several areas such as Area Monitoring, Health Care Monitoring, Environmental and Earth Sensing and Industrial Monitoring. A WSN can be deployed in an unattended hostile environment that is not physically protected. Sensors are used to monitor the environment and the collected data are sent to the base station [1]. Due to their nature, wireless sensor networks are vulnerable to various security threats. Most sensor networks actively monitor their surrounding and it is often easy to deduce information out of the data exchanged between sensor nodes. Such exchange of information leads to leakage of information often resulting in security breaches. Hence, security is a major challenge in wireless sensor networks. Most sensor network routing protocols are quite simple, and for this reason, most of the time, they are more susceptible to network attacks. Some of the vulnerable security attacks in WSN are, Selective forwarding attack, Sinkhole attack, Sybil attack, Wormhole attack, Hello Flood attack, Black hole attack and Node Replication attack [2]. Among these attacks, sinkhole attack is more vulnerable due to the reason that it leads to a variety of attacks.

In a sinkhole attack, an intruder compromises a node or introduces a counterfeit node inside the network and uses it to launch an attack. The compromised node tries to attract all the traffic from neighboring nodes based on the routing metric used in the routing protocol. A sinkhole attack prevents the base station from obtaining complete and correct

ISSN: 1738-9976 IJSIA

sensing data, and thus forms a serious threat to higher-layer applications. Sinkhole attacks are difficult to counter, because routing information supplied by a node is difficult to verify.

Once Sinkhole attack enters into a network, it is capable of performing Selective Forwarding attack, Wormhole attack, Flooding attack, Sybil attack and Black hole attack [3]. Many researchers have proposed several techniques for detecting sinkhole attacks in wireless sensor networks.

There are various optimization problems in Wireless Sensor Network namely, design, deployment, computational complexity and security management. To handle these issues, Heuristic methods are used. Swarm Intelligence is one of the heuristic methods which can be applied for an important security threat in wireless sensor network namely, Sinkhole attack detection effectively.

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).

The main objective of the research work is to detect the sinkhole attack present in wireless sensor network using swarm intelligence techniques. Secondary objectives are to improve the detection rate and packet delivery ratio and to minimize the false alarm rate, message drop and delay.

This section discussed about the wireless sensor networks and sinkhole attack. Rest of the paper is organized as follows: Section 2 provides the review of literature about the Detection of Sinkhole attack using various other approaches. Section 3 explains the proposed methodology. Section 4 discusses the experiments conducted and the results. Section 5 concludes the work with future scope.

2. Related Works

Sinkhole attacks are major threats to wireless sensor networks. Sinkhole attacks are a type of network layer attack where the compromised node sends fake routing information to its neighbors to attract network traffic to itself. Due to the ad-hoc network nature and many-to-one communication pattern of wireless sensor networks, many nodes send data to a single base station. Based on the communication flow in the WSN, the sinkhole does not need to target all the nodes in the network but only those nodes close to the base station.

It is observed that some recent works in sinkhole attack detection use techniques such as Swarm intelligence, Geostatistical model, Redundancy mechanism, Request and reply of sequence numbers, base station and analyzing the network information. They are presented below.

N.K.Sreelaja *et al*. [4] proposed a model to detect a sinkhole attack. This model identifies an intruder in a wireless sensor network using Ant Colony Optimization based approach. The ACO-AD algorithm proposed detects sinkhole attacks effectively and does not generate false positives. The number of searches using ACO-AD algorithm is less when compared to the traditional binary search and sequential search methods.

H.Shafiei *et al*. [5] proposed two techniques to detect and mitigate sinkhole attacks. It provides a centralized approach to detect suspicious regions in the network using geostatistical hazard model. This has been proposed to estimate the energy holes. A lightweight mitigation method is proposed to eliminate sinkholes. The approach successfully prevents traffic flow towards the regions reported as suspicious, thus the rate of packet delivery to those regions is reduced significantly.

Fang-Jiao Zhang *et al*. [6] proposed a redundancy mechanism to detect the sinkhole attack in a network. In case, if there is any suspicious node in the network, messages are

sent to them through multi-paths. The process of path establishment consists of three stages: Route request, Route reply and Route establishment. The detection algorithm is compared with the classical detection algorithm and it is concluded that the proposed algorithm has higher detection rate.

Tejindereep Singh *et al*. [7] proposed a novel algorithm for detecting sinkhole attack. They proposed a solution for sinkhole attack detection in three steps; i) the sender node first requests the sequence number with the rreq message, the node replies with its sequence number through rrepmessage, ii) transmitting node will match sequence number in its routing table. If it matches, then data will be shared; otherwise, it will assign the sequence number to the node, iii) If the node accepts the sequence number then the node will enter in the network; otherwise, it will be eradicated from the network. Two parameters, packet loss and packets received are considered for comparison.

Maliheh Bahekmat *et al*. [8] proposed a novel algorithm for detecting sinkhole attacks in WSN with the help of base station. The Base Station checks data transmission path and keeps the existing nodes in its memory. Whenever it detects the existence of errors in a packet repeatedly, it checks the path and compares the nodes kept in memory with the new path. Hence, the base station detects the malicious node, notifying other nodes and instructs them not to transmit data to the malicious node anymore. This algorithm decreases the packet loss and energy consumption.

Edith C.H.Ngai *et al*. [9] proposed an efficient algorithm to detect the sinkhole attack. The algorithm finds a list of suspected nodes through checking the data consistently. By analyzing the network flow information, the algorithm identifies the intruder in the list. The algorithm is capable of dealing with multiple malicious nodes. The performance of the proposed algorithm is evaluated through numerical analysis and through simulation.

Table 1 shows the comparison of sinkhole attack detection methods.

Table 1. Comparison of Sinkhole Attack Detection Methods

Authors	Techniques	Observations	Year Published
N.K. Sreelaja *et al*.	ACO-AD algorithm is proposed to identify the sinkhole attacks based on nodeids in the ruleset.	Does not generate false positives. Number of searches is less when compared to traditional methods.	2014
Fang-Jiao Zhang *et al*.	Messages are sent to the suspicious node and by evaluating the replies, the malicious nodes are confirmed.	A new perspective in detecting a sinkhole attacks using Multi-path selection.	2014
H. Shafiei *et al*.	A Distributed Monitoring approach has been proposed to detect malicious behavior in the network.	Prevents the traffic flow towards sinkholes and eliminates the threat of sinkholes.	2014
Tejinderdeep Singh *et al*.	Details like Request (rreq) and Response (rrep) for sequence number are used.	After the correction of attack, Packets loss has been decreased and Packets received has been increased	2013
Maliheh Bahekmat *et al*.	Control Packets are sent to BS before transferring the data packets, Data packets are sent in the form of hop by hop counting.	Packet loss is decreased and energy consumption is also decreased.	2012
Edith C.H.Ngai *et al*.	Proposed algorithm finds a list of suspected nodes through checking the data consistency.	Capable of dealing with multiple malicious nodes	2007

It is observed that, so far only Ant Colony Optimization algorithm, one of the Swarm Intelligence techniques is applied for sinkhole detection. Further, not all swarm intelligence methods are explored for sinkhole detection. Hence, Swarm Intelligence techniques namely, Ant Colony Optimization and Particle Swarm Optimization are

applied for sinkhole attack detection. Out of the two, PSO method is found to be efficient in sinkhole attack detection. Hence, the existing PSO is enhanced. Message drop, delay and false alarm rate are important measures that degrade the performance of a wireless sensor network. Hence these metrics are to be considered for the evaluation of the performance of algorithms for sinkhole detection. The proposed method considers these parameters for evaluation apart from detection rate and packet delivery ratio.

3. Methodology

Different intrusion detecting mechanisms in WSN have been introduced and studied by the researchers in order to detect various attacks. The proposed methodology follows heuristic based detection approach.

3.1 Methodology Overview

There are two phases in the research work. In the first phase, wireless sensor network is simulated using NS2 and sinkhole attacks are injected. In the second phase, detection approaches are applied to the wireless sensor network. Ant Colony Optimization and Particle swarm optimization algorithms are applied to the network. Enhanced particle swarm optimization (EPSO) mechanism has been proposed. Finally the performance of ACO, PSO and EPSO are compared and the best algorithm is identified based on experimental results. Figure 1 shows the methodology overview.

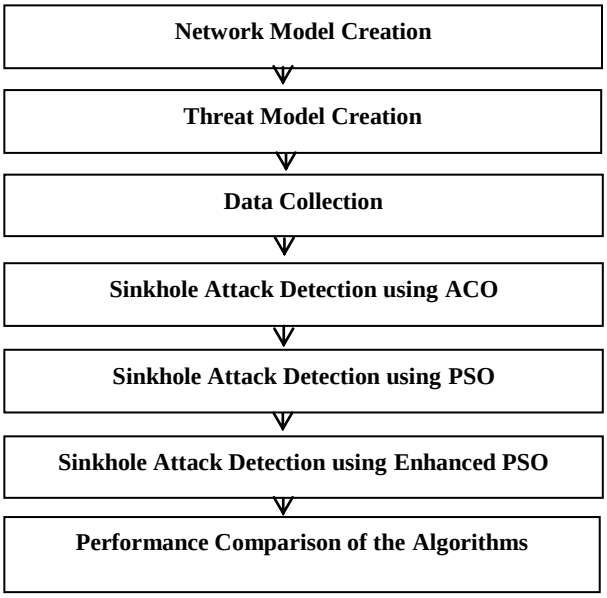

Figure 1. Methodology Overview

3.2 Network Model and Threat Model Creation

For the study of application of Swarm Intelligence techniques, different wireless sensor network scenarios are simulated. This research work uses NS2 to simulate a wireless sensor network scenario. Network sizes ranging from 50 nodes to 250 nodes are considered. Next step is to inject the sinkhole attacks. Number of sinkhole attacks varies upto 10% of the total number of sensor nodes.

3.3 Data Collection

Once the sensor network is established, nodes start communicating with each other. Source node id, Destination node id, Packets sent, Packet received and size of packets are the data collected from the communication between nodes.

3.4 Detecting Sinkhole attacks using Ant Colony Optimization

To detect sinkhole attacks, one of the effective swarm intelligence techniques namely, ant colony optimization is used.

Ant Colony Optimization algorithm (ACO) is a probabilistic technique for solving computational problems which can be reduced to find good paths through graphs. In ACO, ants work in a distributed way with the use of local information; it finds multiple loop-free routes between the source and the destination node [10]. There are three major procedures: establishing the separation procedure, the pheromone updating procedure and the alternative procedure zone to search [11]. Each ant iteratively adds items in a probabilistic way. Each item can be added at most once. An ant's solution construction ends if no item can be added anymore.

Ant colony optimization can be applied in Scheduling problem, Vehicle routing problem, Assignment problem, Set problem and Image processing. Flowchart of ACO is given below in Figure 2.

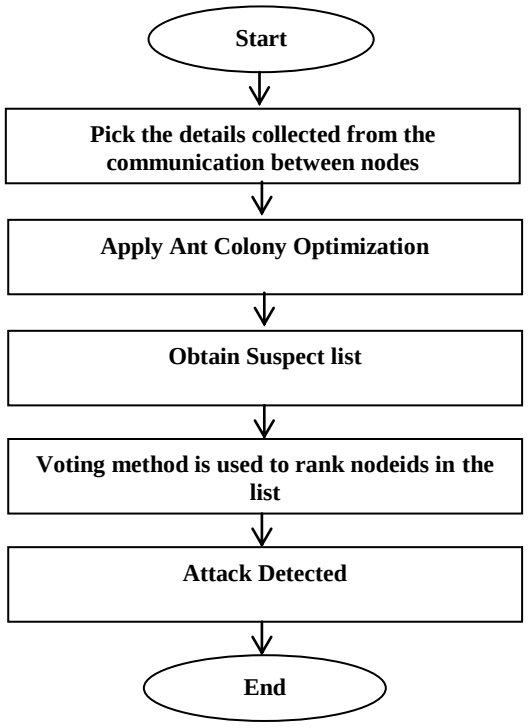

Figure 2. Flow Chart of Ant Colony Optimization

3.5. Detecting Sinkhole Attacks using Particle Swarm Optimization

In this section, sinkhole attack is detected using Particle Swarm Optimization. Particle swarm optimization (PSO) is a population based stochastic optimization technique, inspired by social behavior of bird flocking or fish schooling. Particle Swarm has two primary operators: Velocity update and Position update.

In each iteration, a new velocity value for each particle is calculated. The new velocity value is then used to calculate the next position of the particle in the search space [12].

The PSO algorithm consists of just three steps, which are repeated until some stopping condition is met [13]:

i. Evaluate the fitness of each particle

ii. Update individual and global best fitnesses and positions

iii. Update velocity and position of each particle.

PSO is suitable for solving non-linear optimization problems with constraints.

The movement of a particle x_t at time 't' to time 't+1' is obtained by updating the velocity and position of the particle. The velocity v_t of the particle x_t at time 't' is updated using the formula,

$V_{t+1} = c_1 v_t + c_2.\text{rand1}().(x_t - p_{best}) + c_3.\text{rand2}().(x_t - g_{best})$

where rand1() and rand2() are two random numbers between 0 and 1.

Applications of Particle swarm optimization algorithm are Distributed networks, Electronics and electromagnetics and scheduling. Flowchart of PSO is given in Figure 3.

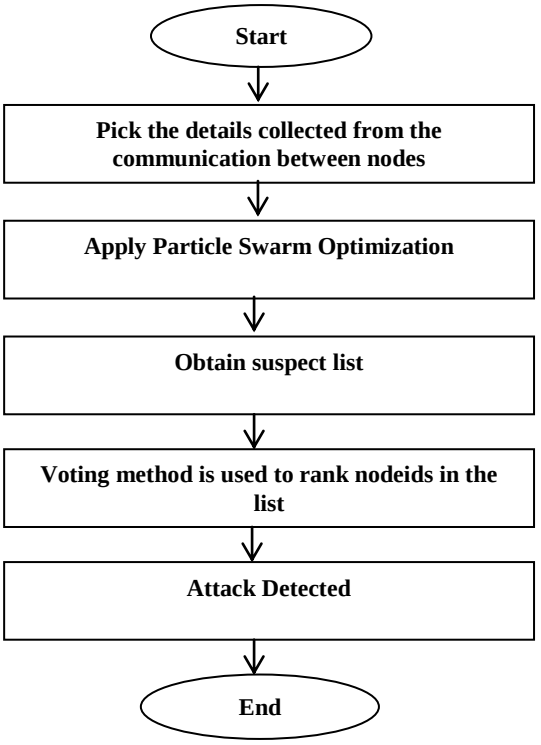

Figure 3. Flow Chart of Particle Swarm Optimization

3.6 Detecting Sinkhole Attacks using Enhanced Particle Swarm Optimization

It is observed that, out of ACO and PSO, PSO method is found to be efficient in sinkhole attack detection. Hence, the existing PSO is enhanced. In this mechanism, hash table are used to obtain more accurate suspect list. Hash table is also used in voting method. Hashing has been previously proposed to record the solutions encountered during recent iterations. All solutions investigated during a search are stored in a list, called solution list. A hash table is used as a pointer to quickly access the solutions stored in solution list. A second list, called collision list is used to store solutions with a hash collision. This mechanism works effectively in detecting attacks. Figure 4 shows the flow diagram of the proposed method. The Pseudo code of Enhanced Particle Swarm Optimization is shown in Table 2.

In PSO, the fitness value is the main variable. To evaluate the fitness value, variables namely g, k, n are initialized. Here 'g' denotes the number of groups, 'k' denotes the number of agents in each group and 'n' denotes the number of

dimensions. Next, nodeids are initialized randomly by the group g and the agent k, $x^{k,g}{}_n$ and $v^{k,g}{}_n$. X and Y denote nodeids. Fitness ^{k,g}(i) denotes the fitness of agent k in the group g at instant i. If this fitness value is the best value found by 'k' in 'g' then, particle best solution $p^{k,g}{}_{best,n}(i) = x^{k,g}n(i)$ will be calculated.

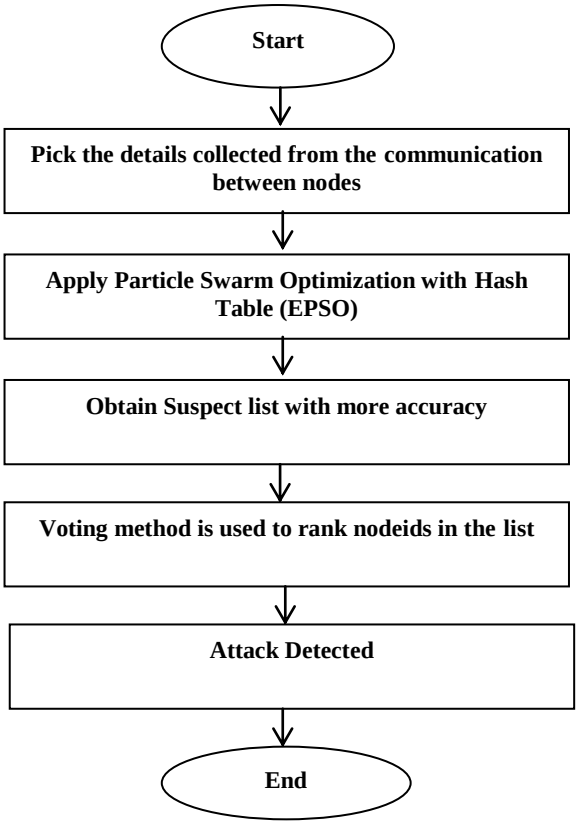

Figure 4. Flowchart of Enhanced Particle Swarm Optimization

Similarly, the fitness value is the best value found by all the agents. After that the global best solution $g^{g}{}_{best,n}(i) = x^{k,g}n(i)$ is calculated. Next, hash table is used. Hash table HT is an integer array. SL denotes the solution list and CL denotes the collision list. By comparing solution list, collision list and ruleset, a list called suspect list is generated which is the input for the next step.

Table 2. Pseudo Code of EPSO

```
Begin
Initialize population;
        While stopping condition not satisfied do
        for j = 1 to no of particles
Evaluate fitness of particle;
Set i=1
        for g=1, number of groups
        for k=1, number of agents in the group
        for n=1, number of dimensions
                Random initialization of x^{k,g}_n
                Random initialization of v^{k,g}_n
          next n
        next k
  next g
do while (Sub boundary case)
```

```
    Flag set global best = FALSE
    for g=1, number of groups
    for k=1, number of agents in the group
            Evaluate fitness k,g(i), the fitness of agent k in group g at instant i
    next k
    next g
for g=1, number of groups
Rank the fitness values of all agents included only in group g
next g
for g=1, number of groups
for k=1, number of agents in the group
    if fitness k,g(i) is the best value ever found by agent k in group g then
            p k,g best,n(i)= x k,g n(i)
end if
    if fitness k,g(i) is the best value ever found by all agents then
          g best,n(i)= xk,g n(i)
end if
next k
next g
i=i+1
if (i >= sub boundaries iterations) then Sub boundary case= FALSE
end do
if (Flag set global best = FALSE) then
Flag set global best = TRUE
Assume d(N)      // hash table implementation
if (h[d(N)]=0) { t=t+1
            h[d(N)]=t and SL[t]= N      //SL-Solution List
            return TRUE}
if (h[d(N)] ≠ 0 and SL[h[d(N)] ] = N) then return FALSE
if h[d(N)] ≠ 0 and SL[h[d(N)] ] ≠ N {
            if N ∉ CL {cl = cl+1          //CL-Collision List
                        CL[cl] = N
                        return TRUE
            }else return FALSE
}
Rank g best,n(i), d[gbest,n(i)]
end if
end
```

All the three algorithms discussed are experimented and the results are presented in the next section.

4. Results and Discussion

4.1. Experimental Setup

Network Simulator 2 is used to create the experimental setup. It supports simulations of TCP and UDP, MAC layer protocols, routing and multicast protocols in Wireless Sensor Networks. Simulation parameters are shown in the Table 3. In this simulated network, standard routing protocol AODV is used. Number of nodes in the network varies from 50 to 250. The Number of sinkhole attacks varies upto 10% of the total number of sensor nodes.

Table 3. Simulation Parameters

Simulation Parameters	Value
Channel Type	Channel/Wireless Channel
Propagation Model	Propagation/TwoRayGround
Medium	Phy/WirelessPhy
Queue Length	Queue/DropTrail/PriQueue
Antenna	Antenna/OmniAntenna
Routing Protocol	AODV
Nodes	50-250
Sinkhole Nodes	5-25

4.2. Performance Evaluation

The parameters used to evaluate the performance of sinkhole attack detection techniques are Detection Rate (DR), False Alarm Rate (FAR), Packet Delivery Ratio (PDR), Message Drop and Average Delay.

4.2.1 Detection Rate: Detection rate is defined as the percentage of correct attacks detected by the total number of attacks present in the network. The formula to estimate the detection rate is,

$$\text{Detection Rate} = \frac{\text{Number of attacks detected}}{\text{Total Number of attacks Present}} \text{ x } 100$$

4.2.2 False Alarm Rate: False alarm rate is the ratio between number of attacks not detected to the total number of attacks in the network.

$$\text{False Alarm Rate} = \frac{\text{Total number of attacks} - \text{number of attacks correctly found}}{\text{Toatl number of attacks}} \text{ X } 100$$

4.2.3 Packet Delivery Ratio: Packet Delivery Ratio is defined as the percentage of number of received packets and the total number of sent packets.

$$\text{Packet Delivery Ratio} = \frac{\text{Number of packets received}}{\text{Number of packets sent}} \text{ x } 100$$

4.2.4 Message Drop: Message drop is defined as the ratio between number of messages not received to the total number of messages.

$$\text{Message Drop} = \frac{\text{Total number of messages} - \text{Number of messages received}}{\text{Total number of messages}} \text{ x } 100$$

4.2.5 Average Delay: Average delay is defined as the ratio between sum of all packets delayed to the total number of packets received.

$$\text{Average Delay} = \frac{\text{Sum of all packets delay}}{\text{Total number of received packets}}$$

The average results obtained from different network scenarios are tabulated in the following table. From the table 4, it is observed that EPSO gives the better results when compared to ACO and PSO.

Table 4. Results Obtained

Metrics \ Methods	Ant Colony Optimization	Particle Swarm Optimization	Enhanced Particle Swarm Optimization
Detection Rate (%)	87.062	88.622	***90.076***
False Alarm Rate (%)	10.648	9.656	***8.472***
Packet Delivery Ratio (%)	78.848	81.178	***83.834***
Average Delay (sec)	7.616	6.086	***5.316***
Message Drop (%)	11.918	9.128	***6.958***

4.3 Results

A sample results for 100 nodes with 10 sinkhole attacks is shown in the following Figures 5 to 11.

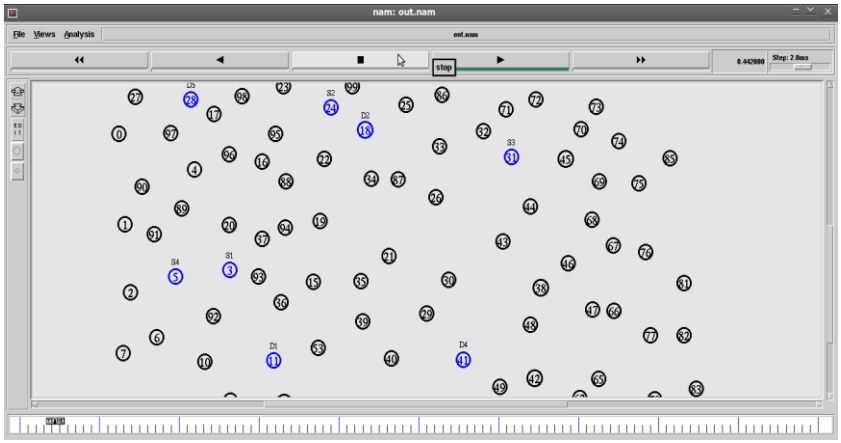

Figure 5. Network Model of 100 Nodes

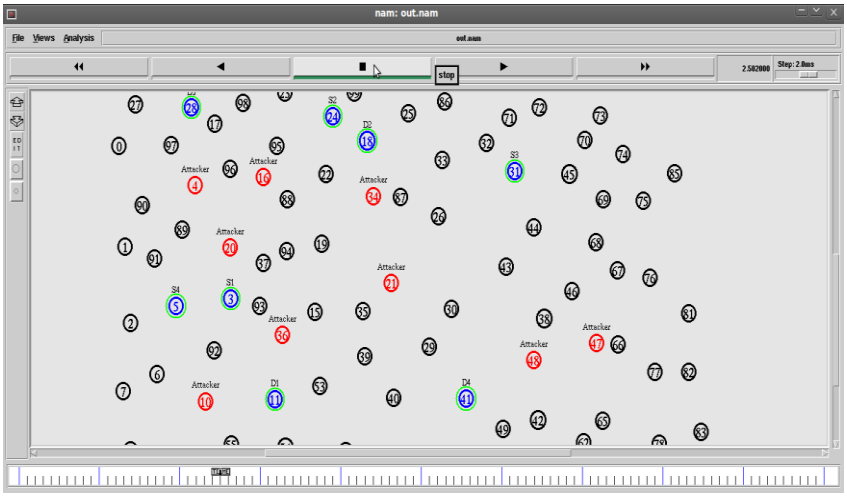

Figure 6. Threat Model with 10 Sinkhole Attacks

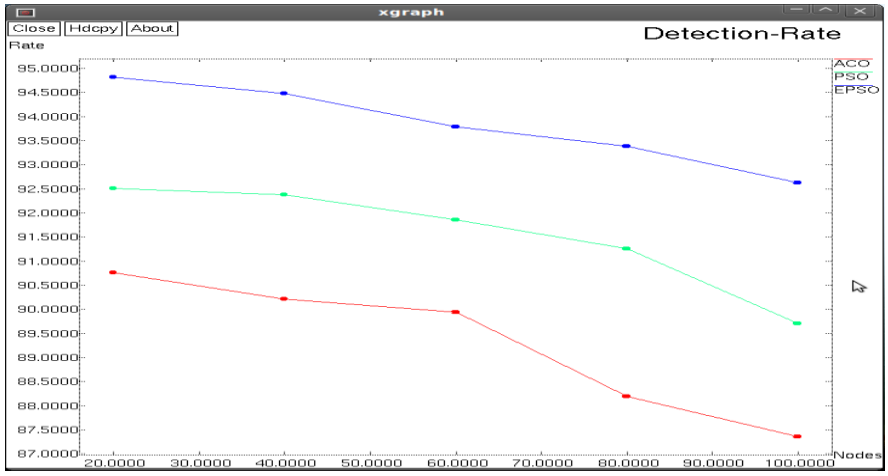

Figure 7. Detection Rate

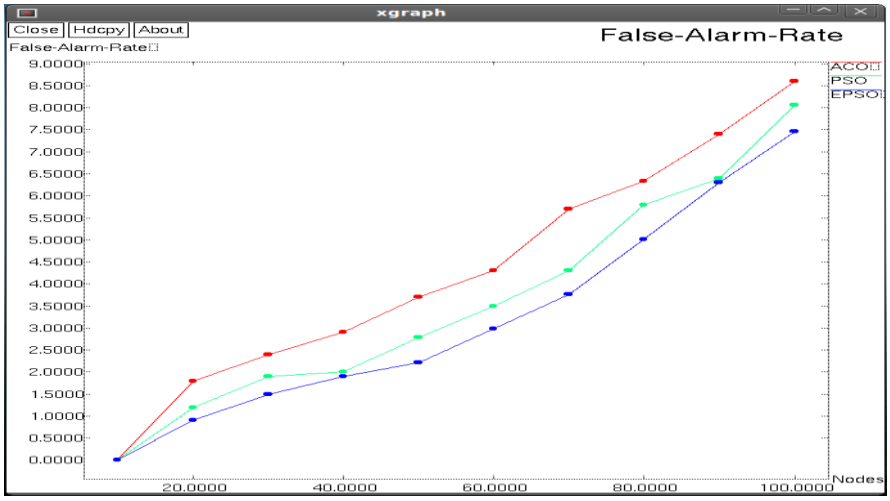

Figure 8. False Alarm Rate

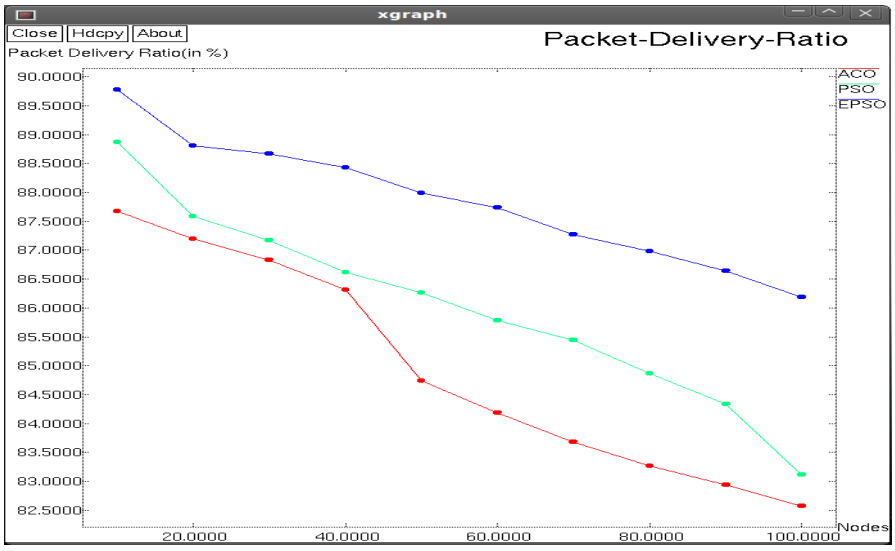

Figure 9. Packet Delivery Ratio

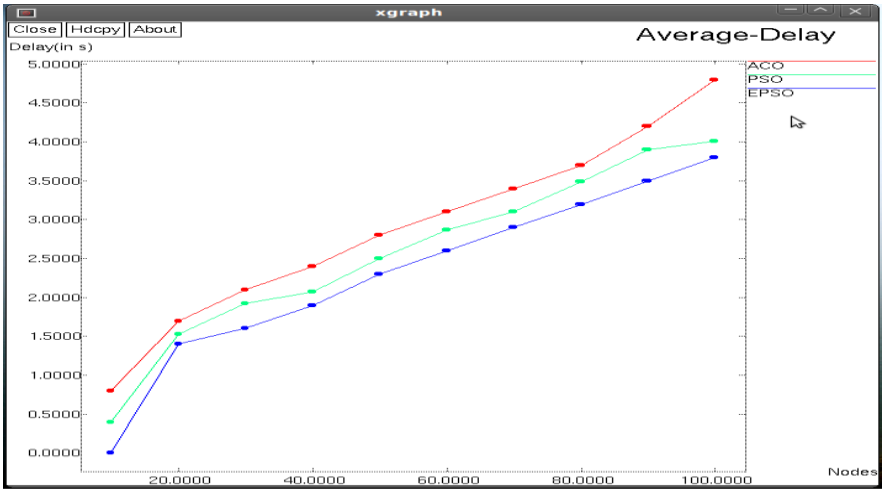

Figure 10. Average Delay

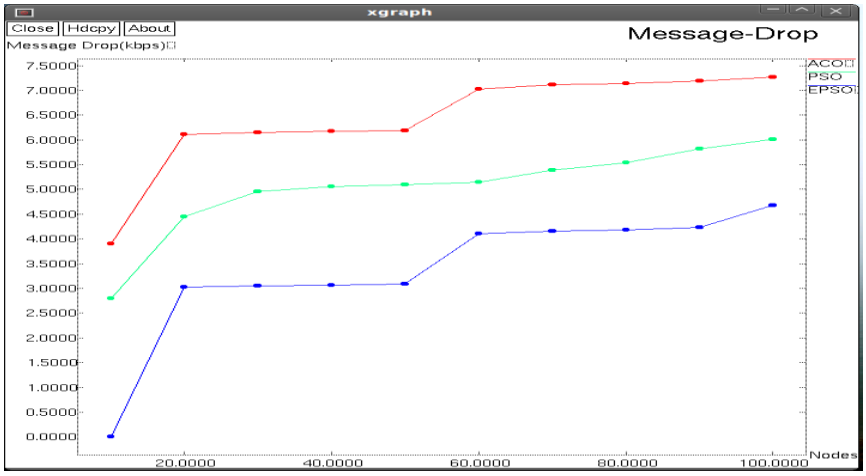

Figure 11. Message Drop

Further, a comparison between ACO and EPSO, PSO and EPSO is done and the results are given in table 5. Detection rate and packet delivery ratio are improved. False alarm rate, message drop and average delay are decreased compared to other two methods.

Table 5. Improvement of EPSO over ACO and PSO

Metrics	Improvement (in %)	
	ACO - EPSO	PSO - EPSO
Detection Rate	3.01	1.4
False Alarm Rate	2.1	1.1
Packet Delivery Ratio	4.9	2.6
Average Delay	2.3	0.7
Message Drop	4.9	2.1

5. Conclusion and Scope for Future Enhancement

Intrusion detection based upon computational intelligence is currently attracting considerable interest from the research community. Swarm intelligence is an effective method used for optimization. The two methods namely Ant Colony Optimization and Particle Swarm Optimization are applied to detect Sinkhole attack in wireless sensor network. An attempt is made to improve the existing PSO using hash table. The method is called Enhanced Particle Swarm Optimization.

In future, other swarm intelligence algorithms like Artificial Bee Colony Optimization, Bees Algorithm, Bat Algorithm, Glowworm Swarm Optimization, Multi-Swarm Optimization can be applied to detect the sinkhole attack.

Swarm intelligence algorithms experimented in this study namely, ACO, PSO and EPSO can be applied to detect other wireless sensor network attacks like Sybil attack, Wormhole attack, Hello Flood attack and Node Replication attack.

References

[1] S. Kumar Gupta, P Sinha, "Overview of Wireless Sensor Network: A Survey", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 1, **(2014)**, pp. 5201-5207.
[2] H Jadidoleslamy, "A Comprehensive Comparison of Attacks in Wireless Sensor Networks", International Journal of Computer Communications and Networks, Vol. 4, Issue 1, **(2014).**
[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] N.K. Sreelajaa, G.A. Vijayalakshmi Pai, "Swarm intelligence based approach for sinkhole attack detection in wireless sensor networks", Elsevier Applied Soft Computing, Vol.19, **(2014)**, pp. 68-79.
[5] H.Shafiei, A.Khonsari, H.Derakhshi, P.Mousavi, "Detection and mitigation of sinkhole attacks in wireless sensor networks", Elsevier Journal of Computer and System Sciences, Vol.80, **(2014)**, pp. 644-653.
[6] F-J Zhang, L-Do Zhai, J-C Yang, X Cui, "Sinkhole attack detection based on redundancy mechanism in wireless sensor networks", Elsevier Procedia Computer Science, Vol. 31,**(2014)**, pp. 711 – 720.
[7] T Singh and H Kaur Arora, "Detection and Correction of Sinkhole Attack with Novel Method in WSN using NS2 Tool", International Journal of Advanced Computer Science and Applications, Vol. 4, Issue 2,**(2013)**, pp. 32-35.
[8] M Bahekmat, MHossein Yaghmaee, ASadat Heydari Yazdi and S Sadegi, "A Novel Algorithm for Detecting Sinkhole Attacks in WSNs", International Journal of Computer Theory and Engineering, Vol. 4, Issue 3, **(2012)**, pp. 418-421.
[9] E C.H.Ngai, J Liu, Mi R. Lyu, "An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks", Elsevier Computer Communications, Vol.30, **(2007)**, pp. 2353–2364.
[10] C Cai, L Yuan, "Intrusion Detection System based on Ant Colony System", Journal of Networks, Vol. 8, Issue 4, **(2014)**, pp. 888-894, April 2013.
[11] D Juneja, Sa Bansal, G Kaur, N Arora, "Design And Implementation of Ear Algorithm for Detecting Routing Attacks in WSN", International Journal of Engineering Science and Technology, Vol. 2, **(2013)**, pp. 1677-1683.
[12] H Saxena, Dr. V Richariya, "Intrusion Detection System using K- means, PSO with SVM Classifier: A Survey", International Journal of Emerging Technology and Advanced Engineering, Volume 4, Issue 2, **(2014)**, pp. 653-657.
[13] A Alsadhan, N Khan, "A Proposed Optimized and Efficient Intrusion Detection System for Wireless Sensor Network", International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering Vol. 7, **(2013)**, pp. 1131-1134.

Authors

G. Keerthana, She received her M.Sc Computer Science degree in 2014 from Avinashilingam Institute for Home Science and Higher Education for Women University, Coimbatore. She is pursuing her M.Phil at Avinashilingam Institute for Home Science and Higher Education for Women University, Coimbatore. Her areas of interest are Network Security, Wireless Sensor Networks.

G. Padmavathi, She is the Professor and Head of computer science Department of Avinashilingam Institute for Home Science and Higher Education for Women University, Coimbatore. She has 27 years of teaching experience and one year of industrial experience. Her areas of interest include Real Time Communication, Wireless Communication, Network Security and Cryptography. She has significant number of publications in peer reviewed International and National Journals. Life member of CSI, ISTE, WSEAS, AACE and ACRS.