ISSN 2347 - 3983
Volume 8. No. 5, May 2020
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter44852020.pdf
https://doi.org/10.30534/ijeter/2020/44852020

Differential Evolution with Artificial Bee Colony Optimization Algorithm based Sink Hole Detection in Wireless Sensor Networks

Sibi Amaran[1], Dr. R. Madhan Mohan[2]
[1]Research Scholar, Department of Computer Science and Engineering, Annamalai University, Chidambaram, India, sibi.amaran@gmail.com
[2]Associate Professor, Department of Computer Science and Engineering, Annamalai University, Chidambaram, India, madhanmohan_mithu@yahoo.com

ABSTRACT

Wireless Sensor Networks (WSN) comprises a group of sensors, commonly employed for data gathering and tracking applications. The design of WSN is prone to the sinkhole attack, where the compromised node tried attracting the network traffic by broadcasting the fake routing updates. An easier authentication process is inadequate preventing WSN from sinkhole attacks as signed routing could also be effortlessly carried out by compromised nodes. To prevent the WSN from sinkhole attack, this paper presents an enhanced artificial bee colony based sinkhole detection (EABC-SHD) algorithm. The EABC-SHD algorithm is based on the foraging behavior of bees and the local optimal problem of ABC has been resolved by differential evolution (DE). Besides, the proposed EABC-SHD algorithm will be executed on the cluster heads, where the choice of CHs is done using a fuzzy logic based mechanism. The clustering process is based on five parameters such as residual energy, distance to BS, distance to neighbors, trust factor and node degree. The proposed EABC-SHD model requires only a minimum amount of time to identify the compromised node, which leads to minimum packet loss and maximum throughput. A detailed simulation analysis is carried out and the results ensured the effective performance of the EABC-SHD algorithm over the compared methods under several aspects.

Key words: Artificial Bee Colony, Clustering, Sinkhole, Swarm intelligence, WSN

1. INTRODUCTION

WSN is a network with inexpensive and elegant computing devices like sensors that is embedded to ecological sensors for measuring temperature, humidity, and so on [1]. It is capable of interacting with one another via the application of wireless radio device. It is composed of massive tiny sensing devices with minimum power, processing, and interaction abilities. The requirement for administration and application of WSN appears due to the unwanted task of maximum sensors in diverse fields. Additionally, encryption and authentication system offer considerable defense for remote-class external attacks [2]. It is due to the existence of an attacker who is permitted to act in the network, provided access by the system and process the autonomous reduction of contents. Such complications can be resolved by applying Intrusion Detection Systems (IDS) which helps in detecting the third party attack [3].

WSN is highly prone to the sinkhole attacks since it is composed with specialized interacting pattern. The sensors observe the target region and transmit the data to base station (BS). The sensor nodes from the similar regions get influence while a node provides maximum quality route to BS. A sinkhole attack is defined as the critical attack which allows the BS to reach accurate and optimal sensing data, and leads to severe risk of higher layer applications [4]. Also, the sinkhole attack cannot be detected very simply as the user authorization and signed routing data is not applicable to eliminate the cooperating nodes from producing signed routing packet with unwanted data. In order to deploy the sinkhole attack, adversary data load from specific region is developed by a compromised node. The adversary often inspires the data traffic by publishing it as it has short route to reach the BS and tampers the packets generated from nodes globally [5].

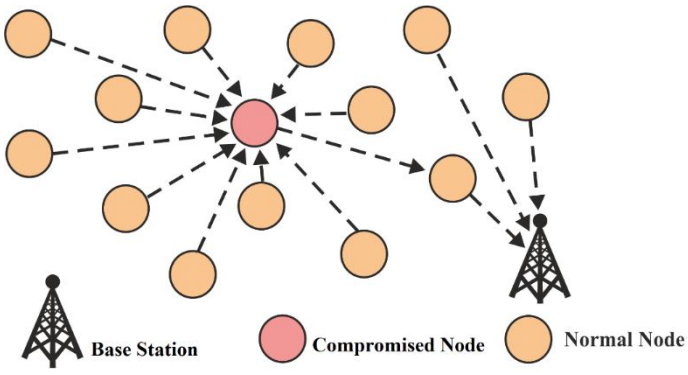

Figure 1: Sample scenario of Sinkhole Attack

Under the sinkhole attack, attacker nodes publicizes the better feasible routes which has minimum hop-distance route to reach the target that attracts the neighbors, thus the published

route has been utilized by the neighbors. Then, the traffic data is forwarded by effective route assigned by sinkhole attacker nodes [6]. Also, a route captivates alternate nodes from the neighboring nodes of sinkhole attacker node that is placed nearby the sinkhole when compared to BS. Hence, the attacker node is comprised with tampering a data, affects the routine network task, and tends to cause severe risk [7]. This type of sinkhole attack is illustrated in Figure 1.

It is moulded with the application of wormhole attack, where the suspicious node holds the packets from corresponding neighbors, and applies a confidential wormhole tunnel for transmitting the packets to other occluded node in WSN, that is used to provide the data to the BS. Thus, it avoids the source from identifying alternate routes that should be greater when compared with 2 hops apart from the BS [8]. When a sinkhole attacker node is developed accurately, then 3 probable paths are emerged namely, messages might be dropped, delay in message transmission, and alteration in messages would be accomplished [9]. Under the application of sinkhole attacker node, messages might be tailored or delayed or lost. It results in severe problems and reduced the performance of WSN, in which the data could not reach the BS with limited duration and alternate network parameters are influenced.

[10] projected a prediction and mitigation of sinkhole attacks in WSN. This type of attacks leads to critical issues in the security of WSN. To eliminate these complexities, developers have presented 2 models for recognition and mitigation of sinkhole attack in WSN. Initially, detection process is relied on the geostatistical hazard approach. The geostatistical method applies remaining energy (RE) of nodes which denotes the severe region on the basis of computed energy. Under the usage of parameter values, the BS present in geostatistical site wish to alleviate the attacks from specific regions. Also, the shared detection model has utilized an expanded map on geostatistical region network in BS. As it is said to be a centralized framework, it has been established with distributed scheme for predicting the sinkhole attack. Here, few nodes were assumed which performs observation of nodes and gives local data regarding the geostatistical system. Secondly, in mitigation method, the malicious area is predicted and removed to prevent sinkhole attack. Once the energy is extracted from BS, the trusted nodes forwards the data with the help of node IDs and it applies secret broadcast over the system. The presented model is mainly used for detecting false-positive nodes. Additionally, the false negative recognition is similar to the number of suspicious nodes that can be identified in geostatistical area. These geostatistical sampling as well as distributed monitoring method has been applied for predicting the sinkhole in a region with maximum energy utilization. Then, the traffic and sinkhole attacks are eliminated.

[11] projected a sinkhole prediction and avoidance technique on the basis of security in WSN. This newly developed method is employed as a basic guidance to select the detection approach to resolve the sinkhole attacks in WSN. It is mainly based on data processing of detection and deployment. This prediction approach depends upon the advanced knowledge as well as prior knowledge free technique. Followed by, it applies the attribute selection, target, detection technique, pattern and security risk in WSN.

[12] proposed a sinkhole prediction method for hierarchical WSN. In the developed method, the SMD, SDP, and SDL nodes are predicted and employed clustering mechanism and every cluster is embedded with effective sensors that are named as cluster head (CH) and it applied for sinkhole attack detection. In the newly deployed model, a novel cluster based approach with powerful CH is applied to predict the sinkhole attacker in hierarchal WSN. Hence, the presented approach examines the classes of sinkhole attacks. [13, 14] applied an automated security investigation according to Machine Learning (ML) models.

[15] implied a discovery and detection model for sinkhole attacks in WSN under the application of clustering approach. It is applied with HEED clustering protocol for detecting the sinkhole in WSN. The CH selection should not be done in a random manner and it is selected on the basis of maximum energy node and realized the presented model with performance measures such as throughput, packet loss and delay. Also, slice model is used to forward the data into tiny pieces and balance slices are encrypted with the application of authentication models in WSN.

This paper presents a new enhanced artificial bee colony based sinkhole detection (EABC-SHD) algorithm. The proposed EABC-SHD algorithm involves a clustering process to select the CHs and construct clusters using 5 input variables. The EABC-SHD algorithm is inspired from the integration of ABC and differential evolution (DE). The foraging behavior of bees has been utilized and the local optimal problem of ABC has been resolved by DE. The proposed EABC-SHD model requires only a minimum amount of time to identify the compromised node, which leads to minimum packet loss and maximum throughput.

2. HYBRIDIZATION OF EABC ALGORITHM

2.1 ABC Algorithm

The ABC model was deployed by Karaboga that is defined as the acceleration of food foraging nature of bees. Here, the food source of the bees is named as solution. It consists of 3 classes of bees such as, employed bee, the onlooker bees, and scout bee. The bee colony is composed with same number of employed as well as onlooker bees. Employed bees find the food source from environment for their hive and save the relevant data in their locations. Then, an Onlooker bee gathers the data from employed bees from the hive for food selection which helps in further nectar extraction. When the nectar amount in food source is minimum, then scout bee explores

fresh food source in a search space arbitrarily. The systematic definition of ABC method is provided in the following:

A. Swarm Initialization

The basic solutions $x_i(i = 1,2,SN)$ of swarm have been produced under the application of uniform distribution as provided:

$$x_{id} = x_{\min d} + rand[0,1](x_{\max d} - x_{\min d}) \quad (1)$$

where x_i denotes the i^{th}significant solution from the swarm, x_{mind} and x_{maxd} are bounds of x_i in d^{th} dimension and $rand[O,1]$ shows an uniformly distributed arbitrary value within the range $[0,1]$.

B. Employed bee phase

Here, every bee shifts towards the direction of alternate solution which is altered as given:

$$v_{id} = x_{id} + \emptyset_{id}(x_{id} - x_{kd}) \quad (2)$$

where, i means the recent solution, k defines randomly decided solution from the SN solutions of a swarm in which $k \neq i$ and d refers arbitrarily selected dimension. φ_{id} denotes arbitrary value within the range of [-1, 1]. Then, the greedy selection has been employed among the present solution to remember the best solution with respect to fitness.

C. Onlooker bee phase

Here, the optimal solution is acquired from their atmosphere. Hence, solutions are chosen according to the probability $prob_i$ for next iteration of novel solutions in the neighborhood. Also, $prob_i$ is determined on the basis of fitness:

$$prob_i(G) = \frac{0.9 \times fitness_i}{\max fit} + 0.1, \quad (3)$$

here $fitness_i$ is the fitness of the i^{th} solution. For the enhanced optimization issue, the $fitness_i$ is same as the objective function value which is same as negative objective function value while reducing the problem. $maxfit$ denotes the fitness of better solution. Once the best solutions were selected, new neighborhood solutions were produced under the application of Eq. (2). Then, greedy selection is used from recent and previous positions to learn the onlooker bees.

D. Scout bee phase

When prefix duration, a solution is not feasible to upgrade itself and it is assumed as best solution and concerned bee is a scout. In ABC, the significant managing parameter has been released named as *limit*. Once the iteration is completed, a solution that is not developed. The bee related with decided solution explores new food source in a search space arbitrarily. Basically, a single scout bee can be reinitialized.

2.2. Differential Evolution (DE)

DE is defined as the population-based optimization algorithm (OA), in which the members of the population are said to be capable solutions that are collectively named as search solutions. DE is composed with EA and SI driven features. Also, it is embedded with evolutionary operators such as mutation, crossover, selection and SI models namely, distance and direction of each solutions that is helpful in searching process. DE contains diverse forms of application to resolve the optimization issue, for instance, it is comprised with several selection approaches for target vector, difference vectors applied in update equation, and crossover operator should be employed. In this work, DE/best/l/bin format of DE is used, that defines the decision of target vector might be an appropriate solution, and '1' refers the number of differential vectors applied, and 'bin' shows that DE would employ binomial crossover [16]. The member of DE population is indicated by a D-dimensional vector $x_l(l = 1,2,D)$. The entire DE process is classified into 3 stages as provided in the following:

- Generation of trial vector
- Offspring production
- Selection among the parents and offspring's for the purpose of future computation.

In addition, Mutation, crossover, and selection are the 3 major operators that are applied for executing the above-mentioned strategies. In DE, with the application uniform distribution, a population with exact size is produced for a search region. Alternatively, to produce upcoming population, a total of three phases are carried out. The crucial and required portion of DE process is that, production of offspring vector that is contributed with 2 operators like mutation and the crossover. At last, greedy selection is deployed among parents and offsprings for selecting optimal vectors so that the next generation might be effective.

3. THE PROPOSED EABC-SHD ALGORITHM

The sinkhole attack can be detected by, every individual CH has IDS, which has been chosen by fuzzy logic mechanism. A set of different modules determines the operation of IDS are Local Packet monitoring, Local detection engine, Cooperative detection and Local Response module. The first module collects the audit data by observing its nearby nodes. depending upon the rules derived for the prediction of sinkhole attack, the local detection engine of every CH holds a ruleset. It includes a set of node ID of its nearby sensor nodes with the link quality of every CH determined utilizing the local packet monitoring system by snooping into the neighbouring node communication [17]. The node ID is arranged in an increasing order. Once a route update packet reaches to a CH, the CH node ID of the route update packet undergo comparison with the node ID in the ruleset saved in the local detection engine. The EABC-SHD relied model is applied for matching the sensor node ID in the ruleset. When the matches are not satisfied with the CH's nodeid, a sinkhole attack is identified and an alarm is raised. A mismatch with the link quality denotes a node impersonate other nodes. The

node raises an alarm and has the suspect list comprising the node ID of input data. The CHs generate an alarm, create a group and the intruder has been determined in a cooperative way. Figure 2 illustrates the model of IDS to identify an intruder resulting in the sinkhole attack.

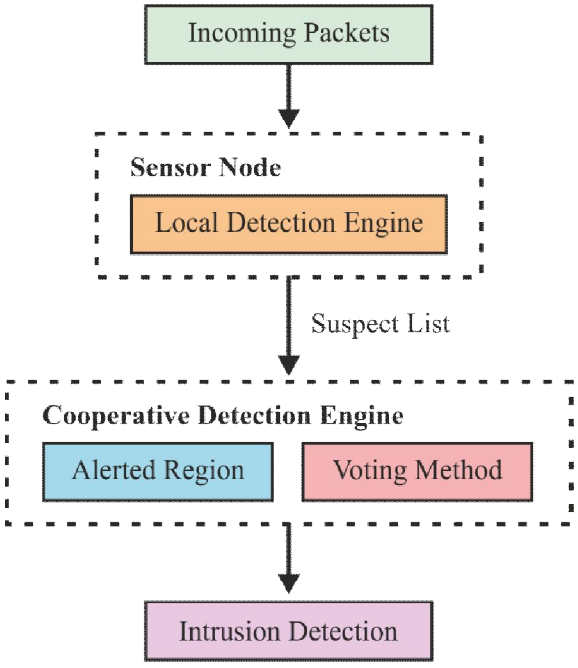

Figure 2: WSN Intrusion Detection System

3.1. Fuzzy logic based Clustering Process

Fuzzy logic (FL) is composed of 4 phases:

Fuzzifying input variables: Transform the accurate input and maps into proper linguistic variable

Membership Functions: Triangular as well as Trapezoidal membership function (MF)

Fuzzy decision blocks: The rule base is defined as the collection of if-then rules that combines the input as well as output fuzzy metrics with the application of linguistic variables.

Defuzzification: It converts the fuzzy output probability to the exact value.

The input attributes as well as linguistic variables are used in the selection of CH. The fuzzy if-then rules used for CH selection and cluster size. A rule has been represented in Eq. (4).

$$\text{Rule}(i)\,\text{IF}\,r_1 \text{is} Y_1^i \text{AND} r_2 \text{is} Y_2^i \text{AND} r_3 \text{is} Y_3^i \text{AND} r_4 \text{is} Y_4^i \text{AND} r_5 \text{is} Y_5^i \text{THEN} s_1 \text{is} Z_1^i \text{AND} s_2 \text{is} Z_2^i \quad (4)$$

where i denotes i^{th} rule present fuzzy rule, Z_1, Z_2,...., Z_5 defines the parallel fuzzy set of r_1, r_2, .., r_5. Rule base is comprised with 243 rules and it is produced on the basis of Madame Inference system that provides best simulation outcome.Centroid of Area (COA) model is applied for defuzzification that is expressed in Eq. (5).

$$\text{COA} = \frac{\int \mu_Y(r).\,r\,dr}{\int \mu_Y(r).\,dr} \quad (5)$$

Once determining the probability of CH selection, every node forwards a CH_CANDITATE_MSG to the neighboring nodes. The message is enclosed with ID and possibility of becoming CH. The nodes accept the message and a node with maximum probability would be elected as CH and publish the state CH_WON to the neighbors. Only few nodes might receive the CH WON from concern neighbors. At this point, the nodes might select the closest CH by transmitting CH_JOIN message. When the message has been received, CH validates the space for novel cluster members (CM). While the CM count is minimum than cluster size, then it receives the new CM by forwarding CM_ACCEPT or CH_REJECT message. The removed node orders the upcoming nearer CH from the existing node and it is followed until it is combined to a cluster. If the CH is not accepted as a CM, then it is named as CH. Thus, no divided nodes would be existed in the system.

3.2. Sinkhole attack detection Process

Swarm intelligence (SI) models in WSN are extensively applied due to the optimal computation and simple implementation. The inclusion of optimization in WSN is because of the maximum dimensionality with respect to count of nodes and difficulty by means of energy resource limitations, etc. The above-mentioned factors of WSN are reported under the application of Optimization Algorithms (OA) and EA are highly important in this model. For the prediction of sinkhole attack using EA model, it plays a minimum role than other methodologies [18].

Each sensor node in WSN seeks for packets obtained on route update request and EABC-SHD approach is applied for detecting the sinkhole node on the basis of rule matching technology. Basically, the artificial bee's works in a colonial manner fashion for the purpose of getting best food source with the application of waggle dance where the superiority of food source has been determined. The productiveness of an artificial bee is described by the fitness measure. The artificial bees are modified into a best solution in a supportive fashion where the employee bee verifies the available food sources randomly and onlooker bees selects the best food source from the acquired food sources of employee bees whereas scout bees find the search space. The waggle dances from the bees indicates the medium of communication among the bees. In EABC-SHD, every bee is allocated to an energy value from the range of negative integer to positive integer and basic value is 0. The higher energy level of every bee is restricted with the overall number of nodes is +1. The positive as well as negative integer intimates the entire number of searching process, which is developed for finding the sinkhole node from previous rule set table.The Sinkhole attack can be predicted by using the bees which have full access to select a node with a chance of becoming a sinkhole node. After completing the node selection, the desired node would be related with node ID that forwards the route update packet.

For example, when a bee selects the node {5} to compare with node ID then it forwards the route update packet and node ID of {5} and corresponding link superiority would be related with it. In particular, a node is identified as sinkhole node and

node {5} and the power value of bee is '0'. Followed by, when a selected node ID is maximum than a node which forwards route update packet, then the concerned bee is declared with energy value 1. For all nodes, a comparison is carried over with +1 till it meets the sinkhole node. When the node ID is minimum compared to the selected node by bee, then the energy value is -1 and it may be reduced gradually till identifying the sinkhole node. When the nodes are selected for comparison, the binary search would be carried out until finding a sinkhole node.

4. PERFORMANCE VALIDATION

The performance of the EABC-SHD algorithm has been tested in the detection of the sinkhole attack on the node ID's in the provided ruleset. The implementation setup comprises Nodeid for every node present in the deployment region, location, and link quality. The performance of the EABC-SHD algorithm has been validated under diverse parameter setup like varying number of sinkhole nodes, node count and simulation time. A set of measures used to determine the results are PDR, packet loss and energy consumption. A sample set of node ID in the ruleset is provided in Table 1. A sample Rule table representing all the sensor nodes are provided in Table 2.

Table 1: Representation of Node ID for Sensor Node

Positions	Node ID	Link Quality
1	65212900007	46
2	65212900076	43
3	65212900093	27
4	65212900148	21
5	65212900721	56

Table 2: Rule set for diverse sensor nodes

Number of Nodes	100,1000,10000
Positions	1…100, 1…1000, 1…10,000
Node Identity (ID)	65212900001… 65212910000

Figure 3 provides a detailed experimental analysis of the EABC-SHD model in terms of PDR under various node count, sink hole nodes, and time. With the application of 100 nodes and 1 sinkhole node in the simulation time of 1000ms, the EABC-SHD algorithm achieves a higher PDR of 0.997 while the other methods namely ABC, ACO-AD and ABC-AD models have attained slightly lower PDR of 0.992, 0.993 and 0.995 respectively. With the existence of 100 nodes and 2 sinkhole nodes in the simulation time of 1000ms, the EABC-SHD algorithm achieves a maximum PDR of 0.995 whereas the other methods namely ABC, ACO-AD and ABC-AD models have attained slightly lower PDR of 0.992, 0.992 and 0.993 correspondingly. Under the application of 100 nodes and 3 sinkhole nodes in the simulation time of 1000ms, the EABC-SHD algorithm attains a best PDR of 0.999 while the other model like ABC, ACO-AD and ABC-AD models have attained slightly lower PDR of 0.982, 0.989 and 0.99 respectively. Similarly, with the employment of 100 nodes and 1 sinkhole nodes in the simulation time of 10000ms, all the EABC-SHD, ABC, ACO-AD and ABC-AD models have accomplished a higher PDR of 0.999. With the presence of 100 nodes and 3 sinkhole nodes in the simulation time of 10000ms, the EABC-SHD ACO-AD and ABC-AD model reached a greater PDR of 0.999 and the other methods namely ABC model have attained slightly lower PDR of 0.998. With the presence of 100 nodes and 3 sinkhole nodes in the simulation time of 100000ms, all the EABC-SHD, ABC, ACO-AD and ABC-AD models have attained a maximum PDR of 1.

Figure4 offers a brief experimental analysis of the EABC-SHD model by means of packet loss under various node count, sink hole nodes, and time. With the existence of 100 nodes and 1 sinkhole node in the simulation time of 1000ms, the EABC-SHD model attains a lower packet loss of 18 while the alternate techniques like ABC, ACO-AD and ABC-AD models have accomplished slightly better packet loss of 31, 29 and 21 correspondingly. Similarly, under the presence of 2 sinkhole nodes in the simulation time of 1000ms, the EABC-SHD model attains a least packet loss of 24 while the other techniques such as ABC, ACO-AD and ABC-AD methodologies have reached slightly higher packet loss of 32, 33 and 27 respectively. With the existence of 100 nodes and 3 sinkhole nodes in the simulation time of 1000ms, the EABC-SHD algorithm accomplished lower packet loss of 36 and other methods namely ABC, ACO-AD and ABC-AD models have attained slightly higher packet loss of 71, 46 and 40 respectively. Likewise, under the existence of 100 nodes and 1 sinkhole node in the simulation time of 10000ms, the EABC-SHD algorithm attains lower packet loss of 16 while the other methods namely ABC, ACO-AD and ABC-AD models have attained slightly higher packet loss of 31, 30 and 21 respectively. Also, with the presence of 100 nodes and 2 sinkhole nodes in the simulation time of 10000ms, the EABC-SHD algorithm reached a least packet loss of 24 while the other techniques like ABC, ACO-AD and ABC-AD approaches have accomplished better packet loss of 32, 33 and 27 correspondingly. Besides, under the employment of 100 nodes and 3 sinkhole nodes in the simulation time of 10000ms, the EABC-SHD algorithm achieves a minimum packet loss of 36 whereas the other models such as ABC, ACO-AD and ABC-AD models have attained slightly higher packet loss of 71, 46 and 40 correspondingly.

On measuring the packet loss rate under the existence of 100 nodes and 1 sinkhole node in the simulation time of 100000ms, the EABC-SHD algorithm achieves a lower packet loss of 16 while the other methods namely ABC, ACO-AD and ABC-AD models have accomplished maximum packet loss of 31, 30 and 21 respectively. With the utilization of 100 nodes and 2 sinkhole nodes in the simulation time of 100000ms, the EABC-SHD algorithm reached a lower packet loss of 24 while the other methods such as ABC, ACO-AD and ABC-AD models have attained slightly higher packet loss of 32, 33 and 27 respectively.

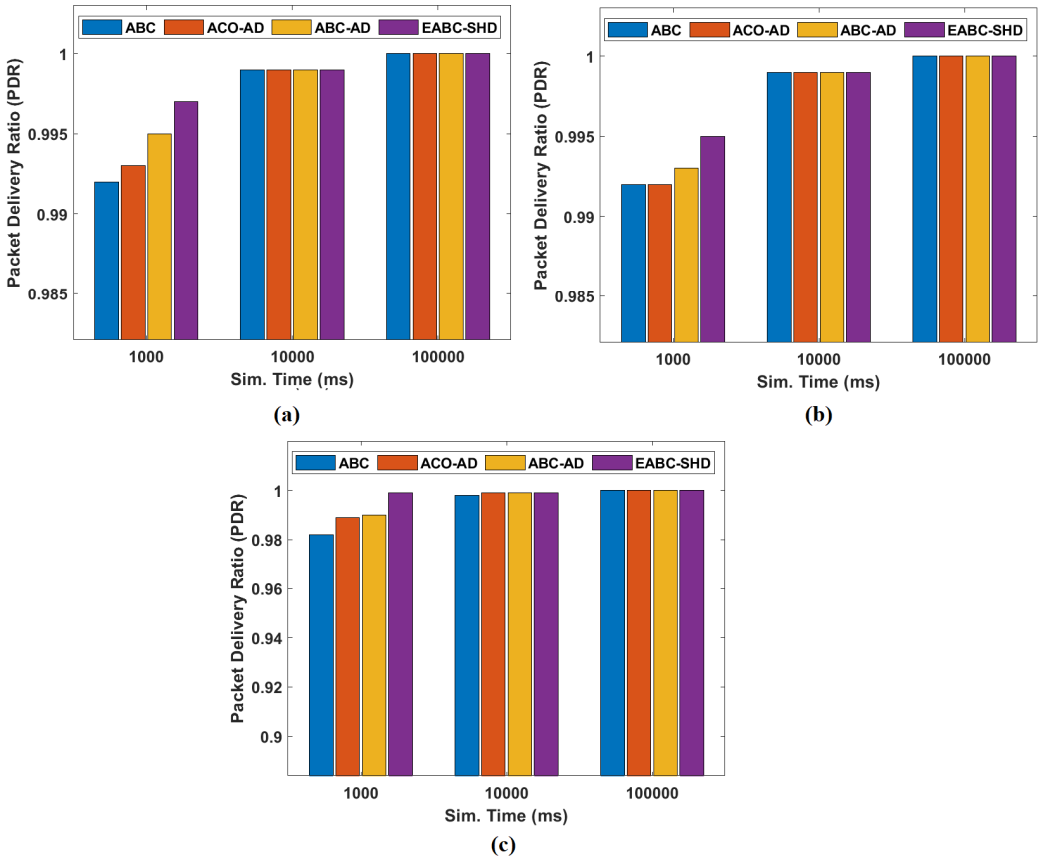

Figure. 3: PDR Graph of 100 nodes a) One sinkhole node b) Two sinkhole nodes c) Three Sinkhole node

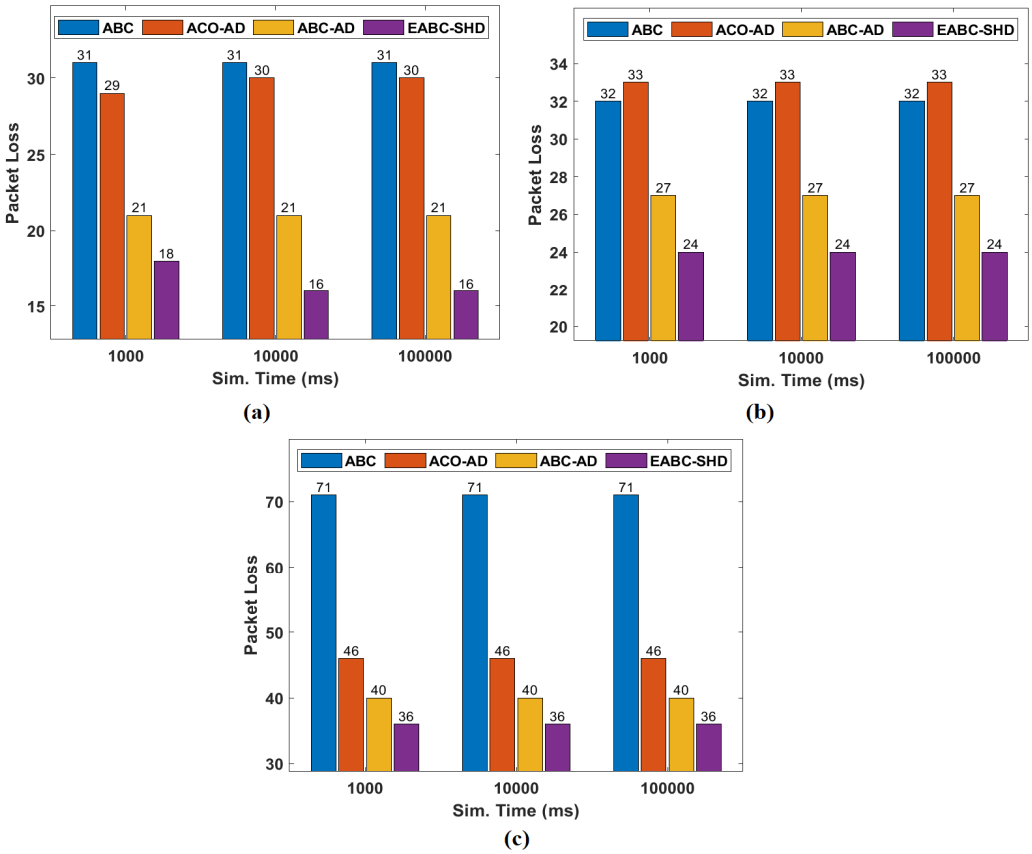

Figure. 4: Packet loss Graph of 100 nodes a) One sinkhole node b) Two sinkhole nodes c) Three Sinkhole node

With the presence of 100 nodes and 3 sinkhole nodes in the simulation time of 100000ms, the EABC-SHD algorithm achieves a minimum packet loss of 36 whereas the other methods namely ABC, ACO-AD and ABC-AD models have attained slightly higher packet loss of 71, 46 and 40 correspondingly.

5. CONCLUSION

This paper has developed a new EABC-SHD algorithm for the identification of sinkhole nodes. The proposed method involves a clustering process to select the CHs and construct clusters using five input variables. The EABC-SHD algorithm is inspired from the integration of ABC and DE. The foraging behavior of bees has been utilized and the local optimal problem of ABC has been resolved by DE. The proposed EABC-SHD model requires only a minimum amount of time to identify the compromised node, which leads to minimum packet loss and maximum throughput. The comprehensive simulation results ensured that the EABC-SHD algorithm is better than other methods in terms of diverse aspects.

REFERENCES

[1] Chandra Sekhar Reddy, N. Purna Chandra Rao Vemuri, Govardhan, A. **An Emperical Study on Support Vector Machines for Intrusion Detection,** *International Journal of Emerging Trends in Engineering Research,* Vol. 7, No. 10, pp. 383-387, October 2019. https://doi.org/10.30534/ijeter/2019/037102019

[2] Rufo I. Marasigan Jr, Alvin Sarraga Alon, Mon Arjay F. Malbog, Joshua S. Gulmatico, **Copra Meat Classification using Convolutional Neural Network,** *International Journal of Emerging Trends in Engineering Research,* Vol. 8. No. 2, February 2020 https://doi.org/10.30534/ijeter/2020/30822020

[3] Subramaniyam, S, **Performance Analysis on Diesel Engine using Neem and Soya Bean Oil,** *International Journal of Emerging Technologies in Engineering Research (IJETER),* Vol. 5, Issue 8, August 2017.

[4] C. Karlof, and D. Wagner. **Secure routing in wireless sensor networks: Attacks and countermeasures**, *Ad hoc networks*, Vol. 1, no. 2-3, 2003, pp. 293-315.

[5] R. Jadhav, and V. Vatsala. **Security issues and solutions in wireless sensor networks**, *International Journal of Computer Applications*, Vol. 162, no. 2, 2017, pp. 14-19. https://doi.org/10.5120/ijca2017913256

[6] E. C. Ngai, J. Liu, and M. R. Lyu. **An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks,** *Computer Communications*, Vol. 30, no. 11-12, 2007, pp. 2353-2364.

[7] H. Shafiei, A. Khonsari, H. Derakhshi, and P. Mousavi. **Detection and mitigation of sinkhole attacks in wireless sensor networks**, Journal of Computer and System Sciences; Vol. 80, no. 3, 2014, pp. 644–653.

[8] A. B. Karuppiah, J. Dalfiah, K. Yuvashri, and S. Rajaram. **An improvised hierarchical black hole detection algorithm in Wireless Sensor Networks,** In *International confernce on innovation information in computing technologies*, February 2015, pp. 1-7. IEEE.

[9] E. C. Ngai, J. Liu, and M. R. Lyu. **On the intruder detection for sinkhole attack in wireless sensor networks,** In *2006 IEEE International Conference on Communications*, Vol. 8, June 2006, pp. 3383-3389). IEEE. https://doi.org/10.1109/ICC.2006.255595

[10] H. Shafei, A. Khonsari, H. Derakhshi, and P. Mousavi. **Detection and mitigation of sinkhole attacks in wireless sensor networks,** J Com - put Syst Sci, Vol. 80, no. 3, 2014, pp. 644–653.

[11] M. Xie, S. Han, B. Tian, and S. Parvin. **Anomaly detection in wireless sensor networks: a survey**, J NetwComputAppl, Vol. 34, no. 4, 2011, pp. 1302–1325

[12] M. Wazid, A. K. Das, S. Kumari, M. K. Khan. **Design of sinkhole node detection mechanism for hierarchical wireless sensor net – works,** SecurCommunNetw, Vol. 9, no. 17, 2016, pp. 4596–4614 https://doi.org/10.1002/sec.1652

[13] K. Vijayakumar, and A. Arun. **Continuous security assessment of cloud based applications using distributed hashing algorithm in SDLC,** ClustComput, Vol. 8, 2017a, pp. 8–9. https://doi.org/10.1007/s1058 6-017-1176-x

[14] K. Vijayakumar, and C. Arun. **Automated risk identification using NLP in cloud based development environments,** J Ambi - entIntell Human Comput, Vol. 8, 2017b, pp. 8–9.

[15] D. B. Vishwas, C. N. Chinnaswamy, T. H. Sreenivas. **Discover and prevent the sinkhole attacks in wireless sensor network using clus - tering protocol,** Int J Adv Res Comput Sci Technol Vol. 2, no. 4, 2016, pp. 26–28.

[16] N. K. Sreelaja, and G. V. Pai. **Swarm intelligence based approach for sinkhole attack detection in wireless sensor networks,** Applied Soft Computing, Vol. 19, 2014, pp. 68-79. https://doi.org/10.1016/j.asoc.2014.01.015

[17] N. Nithiyanandam, and P. Latha. **Artificial bee colony based sinkhole detection in wireless sensor networks,** Journal of Ambient Intelligence and Humanized Computing, 2019, pp. 1-14.

[18] S. S. Jadon, R. Tiwari, H. Sharma, and J. C. Bansal. **Hybrid artificial bee colony algorithm with differential evolution,** Applied Soft Computing, Vol. 58, 2017, pp. 11-24. https://doi.org/10.1016/j.asoc.2017.04.018