Optimizing Fuzzy Adaptive Based Metaheuristics ABC to Detect Malicious Node to improve the performance of WSN

Virendra Tiwari, Dr. Akhilesh A. Waoo

{[1]virentiwari@gmail.com, [2]akhileshoo@gmail.com}

Department of CSE, AKS University, Satna, Madhya Pradesh

Abstract: The Wireless Sensor Networks comprises a set of sensors situated at different locations, usually employed for the gathering of data and tracking applications like monitoring the movement of autonomous nodes in both static and dynamic environments. However, the design of WSN has some the vulnerabilities mainly; its security problems nowadays are found hot research topics in many applications by the researchers. To prevent sinkhole attacks, this paper is doing some research on it and will try to deploy an enhancing and Optimized Artificial Bee Colony algorithm based on fuzzy logic to improve sinkhole detection via packet delivery rate, packet drop, energy exchange, and throughput in a wireless sensor network. Lastly, a simulation using NS2 is performed to evaluate the effectiveness and accuracy by showing initial results and the expected outcome of the proposed model, and the executed simulation result shows that the proposed model could work to some extent.

Keywords: Wireless Sensor Network (WSN), Clustering, Artificial Bee Colony (ABC), Sinkhole Attacks, Swarm intelligence Security.

1. Introduction

With the aid of the internet, Wireless Sensor Networks (WSN) developed on a large scale in recent years play a very important role, in particular, they are used for developing smart sensors [1][2][3][4][5]. Monitoring the environmental distribution of these smart sensors is done geographically in the network. The routing process gathers information from various sensor nodes situated in wireless networks which are carried by multihop and forwarded to the base station [6][7][8][9][10]. Node placement makes it is capable of communicating with each other via applications of wireless radio devices of the network without following any particular or specific structure and it creates an opportunity to place the nodes in a remote area[11][12][13][14][15][16]. Thus this setup requires an efficient algorithm and proper protocol for deploying the sensor nodes in the wireless environment for administration so these nodes could be protected from the various types of unwanted attacks in the wireless network to avoid manipulation of the transmission medium of distributed nodes otherwise attackers can exploit by gaining access and the information transferred within the network

THEETAS 2022, April 16-17, Jabalpur, India

DOI 10.4108/eai.16-4-2022.2318174

[17][18][19][20][22][23][24]. Security attacks due to the network layer can make the network vulnerable and some of the harmful like acknowledge spoofing, sinkhole attack, selective forwarding, Sybil attack spoofed or altered routing, and Wormhole attack [24][25][26][27].

1.1 Metaheuristics and Fuzzy Adaptive Differential Evolution (FADE)

Fuzzy Adaptive Differential Evolution (FADE) is an effective algorithm used for solving various optimization problems in different fields. However, the accuracy of DE depends on the user control parameters, and tuning these parameters after opting for the appropriate parameter value is a challenging task [28]. Therefore this work proposed a novel variant of the differential evolution algorithm to improve the overall performance of the network that asks users to choose a few search parameters instead of based on pre-existing expertise and available observation having fluctuating control elements [29]. The Fuzzy Adaptive Differentially Evolution (FADE) method uses fuzzy logic supervisors to set the probability of mutation and crossover procedures based on changing the parameter exploration which inputs include relative function values [30]. This novel algorithm has the implementation of standard test functions to show the working mechanism that allows these functions to converge more quickly. In our proposed technique, during the initial phase of evolution, we are using the fuzzy DE mutation method which enlarges its search space that aids in finding more promising results to avoid premature convergence. This value of the sigmoid function gets reduced with the increased number of iterations at the subsequent phase of the evolution process [31].

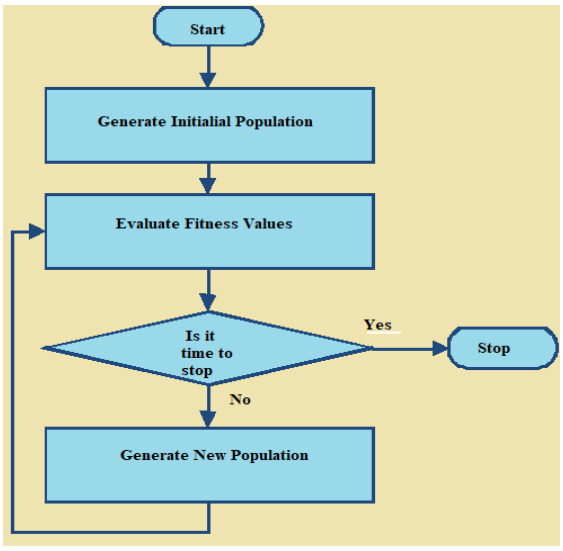

Fig. 1. Fuzzy Adaptive Differential Evolution Method

1.2 Artificial Bee Colony Optimization (ABC)

Artificial Bee Colony Optimization algorithm is swarm-based and bio-inspired, modeled by the intelligent foraging behavior of honey bees in the group for optimizing numerical

problems. The model has three essential components: employed, onlooker foraging bees, and food sources [32]. During the initial phase, half of the colony consists of one kind of employed bee and the next half of another kind of bee which is an onlooker bee [33]. Employed bees search for rich food sources (good solutions for a given problem) within the neighborhood and after determining share new food sources information with onlooker bees [34]. Onlooker bee tries to track the best one from the area of accessible food sources by analyzing received information. Employed bee having abandoned food source becomes a scout and starts a random search for finding a new food source [35]. If the nectar amount of the new food source during evaluation is found higher than the available one, then the employed bee gets switched to the new food source. After completion of all search processes, onlooker bees decide to select the highest probability food source and change the required place of the food source [36].

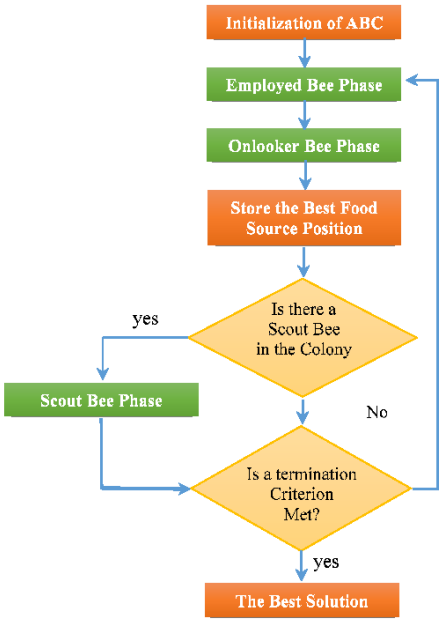

Fig. 2. Artificial Bee Colony Optimization (ABC)

1.3 Wireless sensor Networks (WSN)

Advancement in wireless communication technology has made possible the development of wireless sensor networks comprising of low-cost small size managing devices called sensor nodes that are equipped with temperature, humidity, and other environmental sensors capable of sensing that will communicate with one another via wireless radio devices of the network through radio signals[37]. Proper administration mechanism and technique is required for the robust implementation of WSN [38]. Deployed sensors in the network configure themselves and get connected for exchanging information thereby forwarding the received information to the Base Station [39].

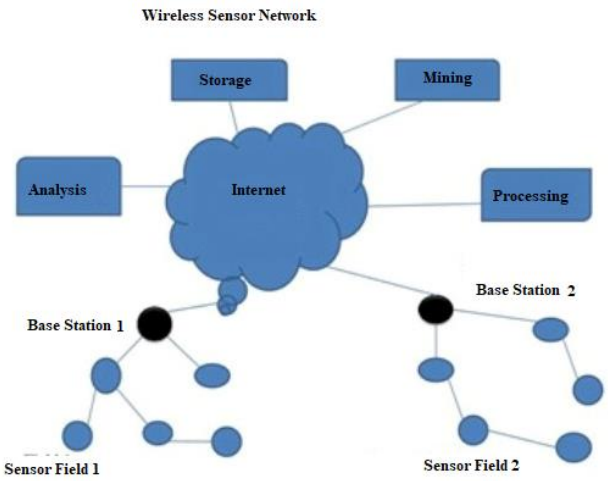

Fig. 3. Wireless Sensor Network (WSN)

1.4 Sinkhole Attack

WSN is vulnerable and susceptible to various forms of malicious attacks among which sinkhole attack has been determined as one of the serious threats carried out by either hacking a device or introducing a fabricated node in the established network [40]. In this type of attack, a fabricated node promotes itself as the best available route(shortest path) to the base station which deceives its neighbor nodes by altering the data to use the route more frequently[41]. Thus, the malicious node in the network has the opportunity to tamper or alter the data, spoil the regular operation or even conduct many further serious challenges to the security of the network [42]. A sinkhole attack restricts the network's base station from receiving complete and authenticated sensor data [43].

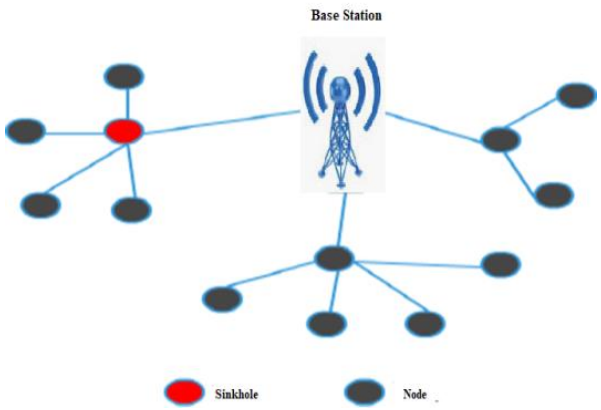

Fig. 4. Sinkhole Attack

2. Related Work

This paper explores one of the most dangerous routing attacks in wireless sensor networks, namely the sinkhole attack by analyzing the literature with prominence on investigating and evaluating available solutions used to assess the WSN's performance. In the below segment, some of the prominent CH selection, Fuzzy adaptive, and optimized ABC methods obtained in the works of literature are being reviewed.

Table 1. Summary of related work

S.no.	Author	Year	Outcomes
1.	N.K. Sreelaja et al. [1]	2014	The given mechanism is agent-based and nature-inspired, which imitates the foraging behavior of bees to identify sinkhole attacks in networks.
2	C.H. Ngai [2]	2007	Given algorithm has been found efficient to detect the list of suspected nodes in the network, with the help of monitoring data consistency by analyzing the network flow information.
3.	Nidal Nasser et al. [4]	2007	Comprehensively studied the concept of enhancing the lifetime of network and security issues addressed consuming much power then proposed routing protocols.
4.	H.Shafiei et al. [5]	2014	A geostatistical hazard mechanism is used as a centralized method for detecting suspicious nodes in the network.
5.	A. Siddiqui et al.[17]	2017	Proposed a technique to detect and avoid wormhole attach based on AODV routing protocol, using the discovery of neighbor and verified path method.
6.	Jing-Zhong Wang et al. [28]	2016	This research proposed an adaptive method based on fuzzy logic for crossover rate (CR) values so the convergence rate of Differential Evolution (DE) algorithms can be improved by deciding two components of the evolutionary environment, calculating the change rate of the solution, and finding the density of each dimension.
7.	R. D, Al-Dabbagh et al. [29]	2014	This study has given a new dynamic parameter that is an identification framework based on FADE to evaluate the CRS A456 robot which is a manipulator of the barycentric parameters.
8.	H. Liu et al.[30]	2014	This research proposes an enhanced GODE method called AGODE, which exercises during evolution an adaptive generalized opposition-based learning (GOBL) mechanism to smartly balance the probability of opposition.
9.	S. Panda et al. [32]	2018	This paper proposes a clustering model of an ABC algorithm to improve the internal dynamics of the cluster head nodes and sensor nodes in the WSN.
10.	Z. Wang et al. [33]	2020	Proposed a clustering algorithm that selects cluster heads using an improved ABC algorithm.

11.	Y. Yue et al. [36]	2016	Proposed heuristic algorithm to jointly consider the selection of cluster head and the routing path from random nodes to the cluster head node of the network, and optimization of mobile sink path planning.

3. Problem Formulation

The deployed sensor nodes continuously collect raw or processed data from the geographically distributed environment and forward it towards the base station of the network in a multihop routing. WSNs have great potential for many applications such as management of disaster, industrial automation, environmental monitoring, target tracking, and medical electronics; However, sensor devices have various limitations such as memory space, limited battery life, expensive, processing capability, and intruder detection. The many-to-one conveying design pattern in sinkhole attacks is undefendable and counted as the most common and one of the challenging issues for a robust wireless network that is carried out in the network layer. The compromised node tries to collect traffic data to prevent the base station from getting complete sensed data from malicious nodes [44]. This study is proposing a novel variant of the optimized ABC algorithm based on FADE for detecting the intruder in a sinkhole attack.

A big amount of investigation and research work by eminent researchers has been already conducted an IoT network has saturation clustering. This concept of determining the sinkhole attacked node in the large network having clustering of with by certain criteria can be a tedious method and not enough efficient because many suspected nodes might not be able to narrow down to identify a particular node. Several models and methods have been opted in the past already to find the optimum option for CHs [47]. This study proposes a model to detect the sinkhole attack and monitoring in the network effectively with an occupied position. This study uses Composites Reputation Value (CRV) for the selection process of CH that depends on a few parameters such as node limit excess energy level and forwarding rate in the network. ABC optimization method is being used to optimize the path length of network CHs, for all the communication, and in this setup, if the CH is identified as a compromised node it influences the entire network communication. Clustering is done using the FADE algorithm in deployed network and every cluster will be associated with nodes such as CH and Inspector Nodes (IN). IN node is set up to take charge as CH if a dead node condition for any CH node arises, after evaluating the present condition of executing communication rotation moves to the next run for the network's CH solution of the setup.

4. Research Methodology

This section of the study describes the proposed methodology below:
Step 1: Clustering using Fuzzy adaptive differential evaluation (FADE)
This section is introducing the FADE method, to improve the performance of Networks. The discussed approach works with n number data points, and each one has d dimensional and a cluster is being denoted by c. A vector comprising numbers is a unique identifier of dimension c×d. All sets are distributed into steady and setup stages using the FADE method [48]. Sensor nodes are found to use less energy when the base station collects all gathered communications from the network CHs as connected with other devices, but they use comparatively more energy when transferring messages to the BS due to being operated in two phases. In the

process of FADE, one node of the organized local cluster serves as the cluster's head with a high strength randomized rotation among the sensors [49]. This feature makes a possible distribution of power utilization across all nodes of the network in a balanced manner, resulting in longer life of the network. FADE, like nearly all other routing protocols, requires safety features and is vulnerable to a variety of risks [50].

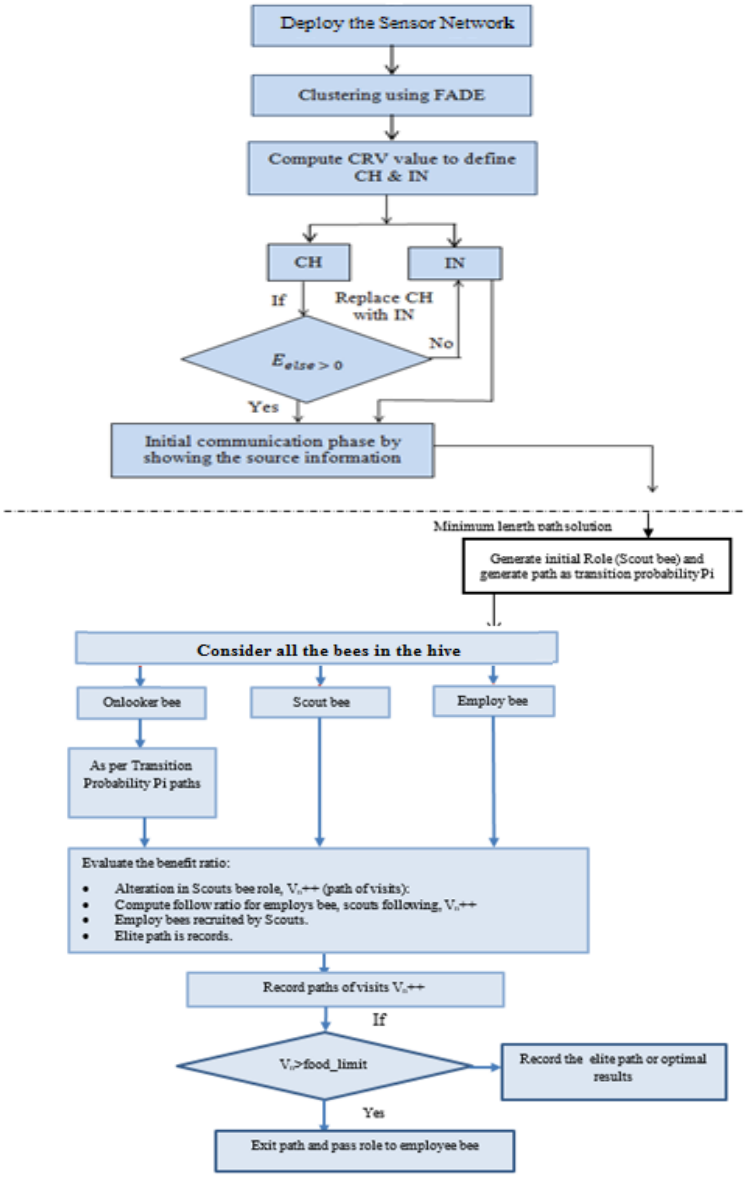

Fig. 5. Research Methodology

Step 2: Calculate the value of Composite reputation Value (CRV) to define CH and IN.

Isomorphic nodes in a cluster are distributed into IN, CH, and MN (Member Nodes). The cluster's radius r0 can be represented as:
r0= R0/2
where R0 symbolizes the network's range of transmission.
A node having the highest CRV value is considered a CH and the following device as an IN.
The CRV numerical of a given node id can be represented:

$$ValC[node_{id}] = x * Pr_{id} + y * \frac{E_{else}}{E_0}$$

Where constants x and y are declared with ranging from 0 to 1 value, and x + y=1. E_0 is an early energy point, E_{else} is an excess power of the nodes, and forwarding rate Pr_{id} for the designated node.

i. IN

The *IN* is trained with some predefined factors preparing a transmission table to keep tracking of all communication by the CH and between other MNs of the network. The constraints include delay time, response time, data loss, time to react, unsuccessful and successful communication, and so on. If IN notices any malicious or suspected activity, it updates throughout the network and intimates the CH and routing table.

ii. CH

CH is responsible for entire system interaction in cluster-based WSN. If the CH is fabricated or compromised, the overall cluster gets set down.

IN gets trained knowledge rules to confirm an “attack” or “no attack” scenario, applied. After identifying, the IN informs the other sensor devices connected in communication and starts acting as the CH for the ongoing information transmission. The routing table gets updated IN and CH by being re-calculated.
After computing the CRV and defining the calculated CH and IN both the sensor nodes will go through the if-else scenario where the proposed study will select the CH node only when the Energy level is greater than Zero and if the level of energy goes down to zero (condition is false) than this method will the IN replace with CH automatically.
Step 3: Now begin transmission by sharing among the nodes by sharing the source information.
Step 4: Create the initial Role of a worker bee (Scout bee) to discover a new spot for the colony to design a hive and set up the path based on transition probability *Pj* and onlooker bee select the food source calculating:

$$P_j = \frac{fitness_j}{\sum_{n=1}^{k} fitness_j}$$

where $fitness_j$ is the fitness function of solution j.
Step 5: Examine all the available bees in the hive using the novel heuristic method ABC algorithm. Positions of food sources suggest different optimization solutions and the amount of connected "nectar".

Step 6: As per the Transition Probability Pi path the selected bees move at this stage according to their source's rate of gaining. By the below equation food resources are further expected to be chosen to have high-level revenue rates:

$$P_j = \frac{ft(X_j)}{\sum_{n=1}^{SN} ft(X_n)}$$

Where $fit(X_j)$ denote the position of the candidate discovered by the employed bee, and $ft(X_n)$ is the solution's fitness rate which is calculated as follows:

$$ft(X_n) = \begin{cases} \frac{1}{f(X_n)} * f(X_n) \ \geq \ 0 \\ 1 + abs\left(f\left(Xn\right)\right), \ f(X_n) \ < \ 0, \end{cases}$$

Where the Xn is the value of objective function $f(X_n)$. The onlooker bees search for sources.
Step 7: Evaluate the benefit ratio whenever the scout bee looks arbitrarily at the path then the variable, gets increments (V_n++).
Elite Path is a searched path taken by the employed bee as the Recorded path.
Step 8: If V_n > FoodLimit, then
pass the role to employee bee, and Exit
If the V_n < FoodLimit,
Record the obtained elite path or optimal outputs by the discussed proposed methodology.

A fuzzy adaptive logic mechanism helps to identify sinkhole attacks using every individual CH ID'S. IN determines the operation of IDS such as Local Packet monitoring, and Local Response module. The network's node ID is stored by arranging in increasing order. Once an update of a routed packet is received to a CH, It goes to get compared with the node ID in the saved ruleset of the local detection engine. The proposed model is based on applying the mechanism of matching the ID of the network's sensor node in the saved ruleset. When the applied matches are not found satisfied with the node id of CH's, a sinkhole attack is recognized with an alarm is raised. A mismatch denotes a node is trying to impersonate other nodes of the network. The CHS would be giving an alarm, and the intruder has been determined. An adaptive fuzzy-based controller is proficient in learning from processed data as well as capable to incorporate linguistic data. Such significant benefits make them much-needed candidates for advanced technology. A smart adaptive fuzzy controller is capable to generate a set of fuzzy control rules automatically and improvement on them can be done as the control process evolves.

5. Simulation-Based Implementation, Experimental Results, and Observations

In this experimental setup of sensors, we evaluated the performance of the proposed method using the network simulator (NS2) with defined parameters of the simulation used in the given table.
Step 1: To carry out the performance evaluations of the proposed model deploying the network in the monitoring area.

Step 2: Clustering using Fade - FADE is an algorithm for WSNs having low-energy hierarchical routing which runs on distinct rounds and all the created set of nodes are distributed into two stages: steady and setup state.
The base stations start receiving gathered communications from the CHs of the network as they get connected with other nodes, sensor nodes use a slight amount of energy, but during message transmission to the BS, they consume more energy. As a result here, the use of the FADE method consumes less energy by implementing it in two different rounds and phases. FADE process, the nodes are organized into a local cluster, having one node as the cluster's head.

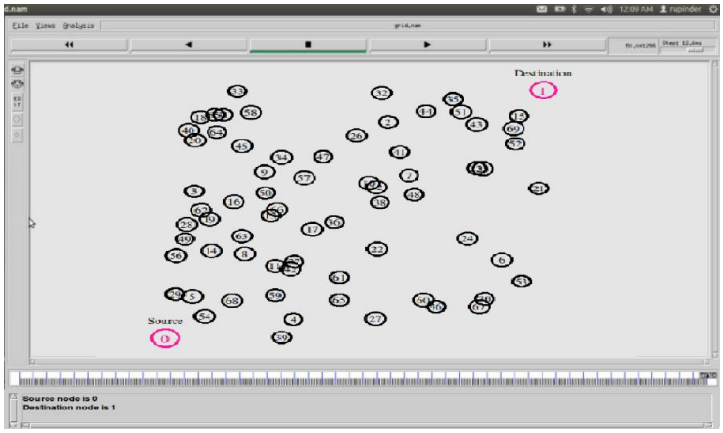

Fig. 6. Before any attack

The performance of the proposed model is being tested by the ability of the algorithm to identify sinkhole attacks based on node ID in the provided ruleset table. The implementation simulation setup comprises Nodeid for every deployed and connected node in the network. The performance of the algorithm has been evaluated under different parameter setups such as determining the number of sinkhole nodes, PDR, energy consumption, and loss of packets.
The obtained results in output are showing that the proposed fuzzy adaptive DE mechanism is efficient to recognize the fabricated nodes in the network with a higher positive ratio and lower false-positive rate.

Table 2. Parameters Value

Simulator used	NS 2.3
Number of nodes	50
Area (meters)	1600×1000
Channel type	Wireless
Routing protocol	LEACH
The initial energy of nodes	512 bytes
Packet size	512 bytes
Deployment Method	Random

We first establish a network by creating the base station (BS) and clusters with each one having a cluster head (CH). Figure 6 provides a situation in the network having nodes 68 and 69 fabricated that could be responsible to drop packets and is identified as the sinkhole attack by the proposed model. These malicious attacked nodes are isolated from the established network for the normal function of WSN.

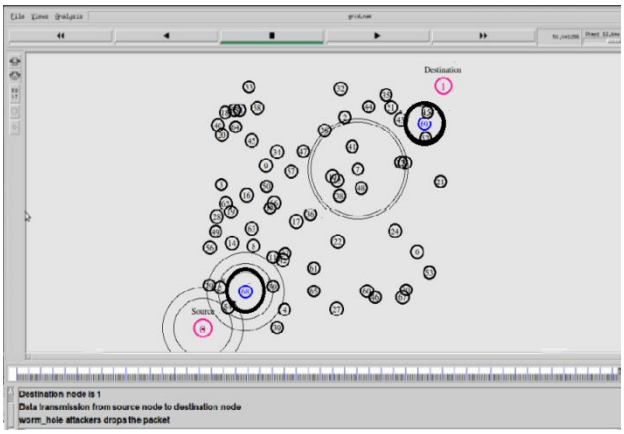

Fig. 7. After sinkhole attack

Packet Delivery Ratio :
Packet delivery ratio (PDR) can be defined as the ratio of the total of received packets at the destination node to the total packets delivered by the source node. PDR is calculated as PDR= (Packets received)∗100/packets generated.

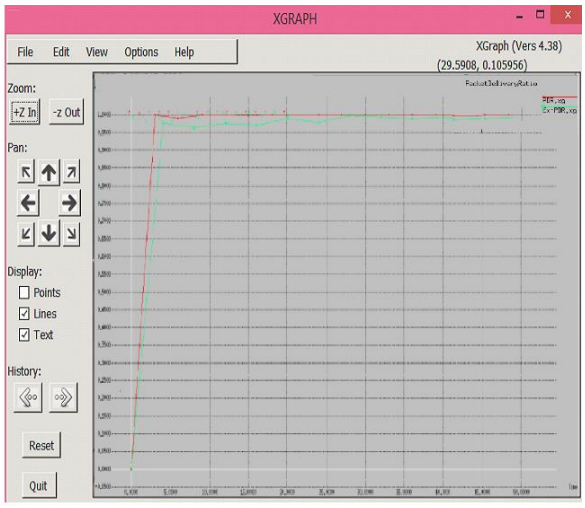

Fig. 8. PDR

Figure 8 shows the analysis of PDR in the scenario of under attack and after implementation of the proposed model increasing PDR after the results of the isolating attack. Increasing the PDR value is a clear indication that there is comparatively less packet loss in the network.

Energy Consumption:

At the beginning of the simulation for the energy computation, we tune the initial value of sensor nodes by 20 joules. In the simulation, energy is termed initial energy and the variable energy in a sensor node is representing the energy level for a specified time duration. The initial energy value is set to pass as an input argument. A sensor node for every packet communication means sending and receiving is expected to lose some amount of energy. Thus the initial energy value gets decreased in the result. The sensor node's energy consumption level of the simulation at any time is determined by calculating the difference between the initial energy and current energy value. If an energy level at any time reaches zero, the node can't send or receive further packets. In the figure, it is shown that the method reduces the consumption of energy as compared to the scenario of attack.

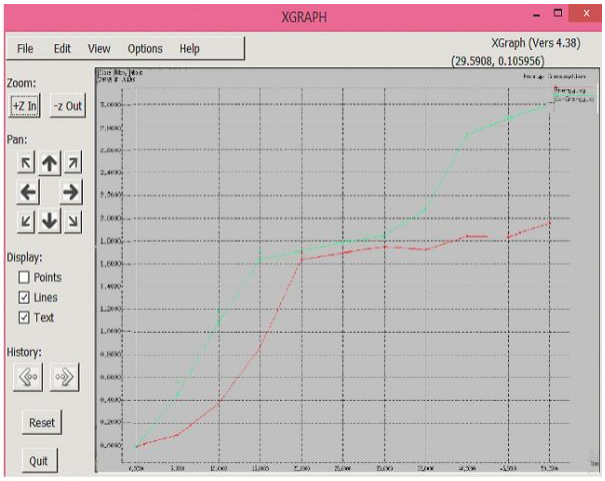

Fig. 9. Energy Consumption

Packet loss is calculated as

Packet Loss = total generated packets− total received packets.

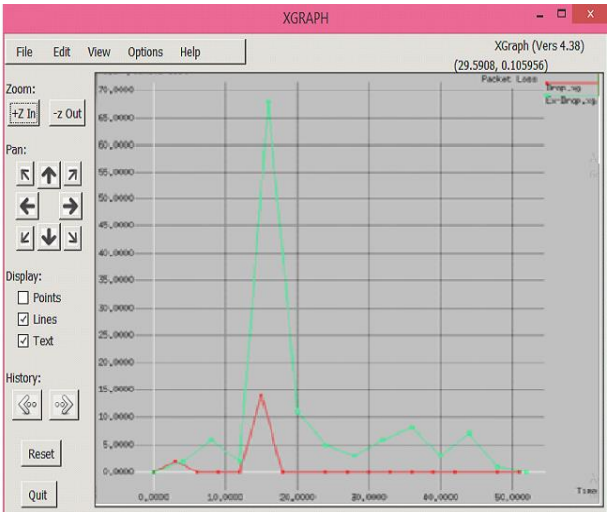

Fig. 10. Packet Loss

Packet loss analysis is shown in the figure in case of under attack and after implementing the proposed method which clearly shows the reduction in packet loss after isolating the attacks. It indicates a high PDR value in the network.

Observation

The estimation of the routing phase of a packet for every network's connected node is determined by using the total energy consumption of a node for all communication components such as transmission, forwarding, receiving, and idle. Different algorithms for a sinkhole node problem LEACH, standard PSO, and used to the enhancement of the energy consumption of results are compared.

The swarm-based ABC algorithm named FADE-based an Artificial Bee Colony is proposed to handle above discussed issues, the parameters represented in the shown figures illustrate many network loads using LEACH. The performance parameters such as packet delivery ratio(PDR) and energy consumption by sinkhole node are displayed in Figure 9.

1. The first algorithm is LEACH of WSN which is known as energy-efficient even though it lacks in some criteria i.e. if the node is not deployed appropriately, it is observed that finding the optimal placement for the node could be struggling with the loss of energy and the more energy consumed by present SH. The network's energy consumption is found almost NIL in the absence of sinkhole nodes.
2. In The next method PSO finds appropriate positions for deploying a node, but the finding of the fabricated node is not efficient in terms of time. This swarm optimization-based technique is comparatively better than LEACH, but the energy consumption level keeps changing not static which depends on some parameters like the network load and the number of nodes.
3. The proposed method is capable to discover the optimal path for placing the node. The LEACH method couldn't identify the sinkhole node quickly and end up with the consumption of more energy by the sinkhole node and spoiled message communication. The second mechanism Particle Swarm Optimization (PSO) able to find the optimal path easily. But the PSO faced difficulty to decrease the SH node consumed energy. But the proposed technique

can create an optimal placement and path for transmission and message communication among the nodes efficiently.

The forwarding of messages is securely carried and the energy consumption by SH is found comparatively less. The delivery of packets is one of the crucial factors in WSN, where the simulated and compared methods(LEACH and PSO) are not found efficient to recognize the sinkhole node quickly. This study helps to enhance the PDR by detecting the SH node at an early stage. The network load and the energy consumption factors by SH node are found less when FADE-based ABC is deployed in the network. The studied technique is observed to reduce the loss of packet, where both the other two methods found fail. The proposed model can decrease the packet loss by identifying the SH node quickly and isolating that specific node from the message communication track in the network.

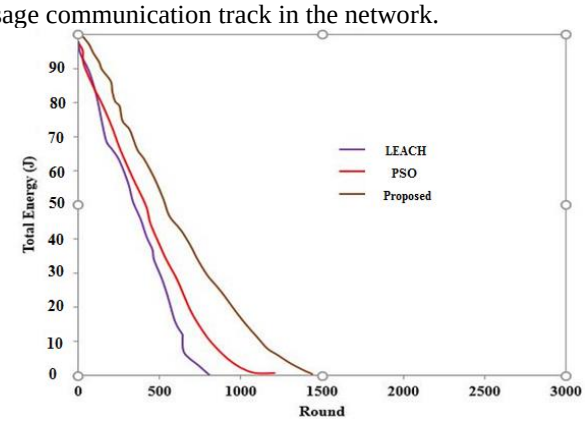

Fig. 11. Sum of energy with 75 sensors.

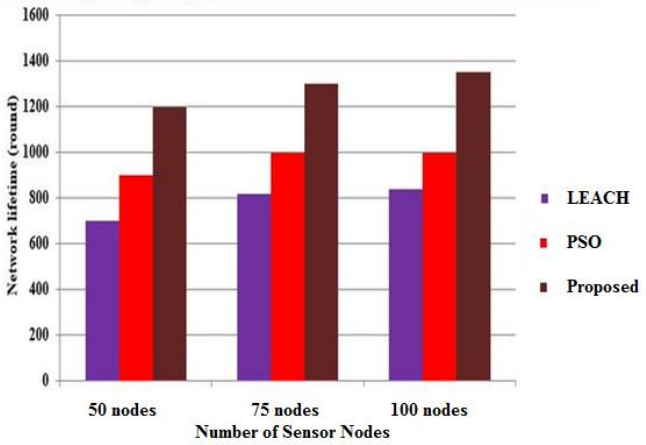

Fig. 12. Lifetime metrics

6. Conclusions

In this paper, the main contribution is to develop a secured new optimized ABC algorithm based on the FADE method for the identification of sinkhole nodes and saving the network from the compromised node by intimating the right information to the base station and the estimated node changed position should be monitored continuously. The proposed mechanism has the process of clustering to select the CHs and make clusters using discussed input variables. The proposed algorithm is inspired by the coalescing of ABC and fuzzy DE. The proposed mechanism helps the working network to find the sinkhole attack. The above-displayed figures are showing that the proposed method is resolving the local optimal problem of ABC by utilizing the foraging nature of bees and the fuzzy DE to effectively outline various methods such as LEACH and PSO requiring only a minimum amount of time to find the fabricated node, which leads to minimum loss of packet and maximum throughput and simulation has also ensured the feasibility of the approach in terms of diverse aspect.

References

[1] Sreelaja,N.K., Vijayalakshmi, G.A., "Swarm intelligence based approach for sinkhole attack detection in wireless sensor networks", Applied Soft Computing 19 (2014).

[2] Edith C. H. Ngai, Liu, J. and Michael R. Lyu; “On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks” IEEE International Conference on Communications, Volume 8, pp. 3383-3389, (2006).

[3] Ramson, S. R. J, and Moni, D. J. "Applications of wireless sensor networks — A survey," 2017 International Conference on Innovations in Electrical, Electronics, Instrumentation and Media Technology (ICEEIMT), 2017, pp. 325-329.

[4] Nasser, N., Chen, Y. "SEEM: Secure and energy-efficient multipath routing protocol for wireless sensor networks" Computer Communications 30 (2007).

[5] Shafiei, H., Khonsari, A., Mousavi, P. "Detection and mitigation of sinkhole attacks in wireless sensor networks" Journal Of Computer And System Sciences 80 (2014).

[6] Fabrice Le Fessant, Antonis Papadimitriou, Aline Carneiro Viana, Cigdem Sengul, Esther Palomar, "A sinkhole resilient protocol for wireless sensor networks: Performance and security analysis”, Computer Communications 35 (2012).

[7] Kaur, L., Kumar, D., "Optimization techniques for Routing in Wireless Sensor Network", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3), 2014, 4719-4721.

[8] Seyed Mahdi Jameii and Seyed Mohsen Jameii, "Multi-Objective Energy Efficient Optimization Algorithm For Coverage Control In Wireless Sensor Networks", International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol.3, No.4, August 2013.

[9] Talwar, M., "Energy Efficient Algorithms For Wireless Sensor Network: A Survey", Indian J.Sci.Res. 11 (1): 082-087, 2015.

[10] Kirankumar Y. Bendigeri and Jayashree D. Mallapur, "Energy Aware Node Placement Algorithm for Wireless Sensor Network", ISSN 2231-1297, Volume 4, Number 6 (2014), pp. 541-548.

[11] Muhammad Saleem, Gianni A. Di Caro, Muddassar Farooq, "Swarm intelligence based routing protocol for wireless sensor networks: Survey and future directions", Information Sciences Information Sciences 181 (2011) 4597–4624.

[12] Sathyamoorthi, T., Vijayachakaravarthy, D., Nandhini, M. "A Simple And Effective Scheme To Find Malicious Node In Wireless Sensor Network", IJRET: International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308.

[13] T. Nidharshini, V. Janani, "Detection of Duplicate Nodes in Wireless Sensor Networks Using Sequential Probability Ratio Testing " International Journal of Advanced Research in Computer and Communication EngineeringVol. 1, Issue 10, December 2012.
[14] Gurjot Singh, Er. Sandeep Kaur Dhanda "Performance Analysis of Security Schemes in Wireless Sensor Network" International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 8, August 2013.
[15] Mayuri P. Kawalkar, Dr. S.A.Ladhake, "An Approach towards Improving the Lifetime and Security in Wireless Sensor Network", International Journal of Computer Science and Information Technologies, Vol. 5 (2), 2014, 2604-2611.
[16] Parmar Amish, V. B.Vaghela "Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV protocol", 7th International Conference on Communication, Computing and Virtualization 2016 Procedia Computer Science 79 (2016) 700 – 707.
[17] Siddiqui, A., Karami, A. and Johnson, M. O. 2017. A Wormhole Attack Detection and Prevention Technique in Wireless Sensor Networks. International Journal of Computer Applications. 174 (Art. 4).
[18] Wei-Lun Chang, Deze Zeng, Rung-Ching Chen, and Song Guo "An Artificial Bee Colony based Algorithm for Power-Efficient Packet Roaming in WSNs".
[19] Patel Nakul"A Survey on Malicious Node Detection in Wireless Sensor Networks"International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064.
[20] Dinesh K. R, Kavitha Bai, A. Rosline Mary" A Survey on Malicious Node Detection in Mobile Access WSN under Byzantine Attacks " International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459 (Online), Volume 5, Special Issue 2, May 2015).
[21] Ali Peiravi, Habib Rajabi Mashhadi and S. Hamed Javadi " An optimal energy-efficient clustering method in wireless sensor networks using multi-objective genetic algorithm " International Journal Of Communication Systems Int. J. Commun. Syst. 2013; 26:114–126.
[22] R.S. Raghav, Sujatha Pothula, Dhavachelvan Ponnurangam, "AN ENRICHED ARTIFICIAL BEE COLONY (EABC) ALGORITHM FOR DETECTION OF SINKHOLE ATTACKS IN WIRELESS SENSOR NETWORK", IJMET, Volume 8, Issue 8, August 2017, pp. 193–202.
[23] Hongjun Dai, Yu Liu, Fenghua Guo and Zhiping Jia, "A Malicious Node Detection Algorithm Based on Principle of Maximum Entropy in WSNs " Journal Of Networks, Vol. 7, No. 9, September 2012.
[24] Tejinderdeep Singh and Harpreet Kaur Arora, “Detection and Correction of Sinkhole Attack with Novel Method in WSN Using NS2 Tool” International Journal of Advanced Computer Science and Applications(IJACSA), 4(2), 2013.
[25] Dr.S.Rajaram, A. Babu Karuppiah, K. Vinoth Kumar " Secure Routing Path Using Trust Values For Wireless Sensor Networks" International Journal on Cryptography and Information Security (IJCIS), Vol. 4, No. 2, June 2014.
[26] Shio Kumar Singh, M P Singh, and D K Singh, "Routing Protocols in Wireless Sensor Networks –A Survey " International Journal of Computer Science & Engineering Survey (IJCSES) Vol.1, No.2, November 2010.
[27] Wang, T., "Traffic Analysis & Modeling in Wireless Sensor Networks and Their Applications on Network Optimization and Anomaly Detection "Network Protocols and Algorithms ISSN 1943-3581 2010, Vol. 2, No. 1.
[28] Jing-Zhong Wang and Tsung-Ying Sun, "Adaptive CR values with fuzzy inference system for differential evolution algorithm," 2016 IEEE Congress on Evolutionary Computation (CEC), 2016, pp. 3162-3169.
[29] Rawaa Dawoud Al-Dabbagh, Azeddien Kinsheel, Saad Mekhilef, Mohd Sapiyan Baba, Shahaboddin Shamshirband, System identification and control of robot manipulator based on fuzzy adaptive differential evolution algorithm, Advances in Engineering Software, Volume 78, 2014, Pages 60-66, ISSN 0965-9978.

[30] Huichao Liu, Zhijian Wu, Hui Wang, Shahryar Rahnamayan, Changshou Deng, “Improved Differential Evolution with Adaptive Opposition Strategy”, CEC- July 6-11, 2014.
[31] Pan, Q., Tang, J., Wang, H. et al. SFSADE: an improved self-adaptive differential evolution algorithm with a shuffled frog-leaping strategy. Artif Intell Rev (2021).
[32] S. Panda, S. Srivastava, S. Mohapatra, and P. Kumar, "Performance analysis of wireless sensor networks using artificial bee colony algorithm," 2018 Technologies for Smart-City Energy Security and Power (ICSESP), 2018, pp. 1-5.
[33] Z. Wang, H. Ding, B. Li, L. Bao and Z. Yang, "An Energy Efficient Routing Protocol Based on Improved Artificial Bee Colony Algorithm for Wireless Sensor Networks," in IEEE Access, vol. 8, pp. 133577-133596, 2020.
[34] Ozturk C, Karaboga D, Gorkemli B. Probabilistic dynamic deployment of wireless sensor networks by artificial bee colony algorithm. Sensors (Basel). 2011;11(6):6056-6065.
[35] Ankit Gambhir, Ashish Payal, Rajeev Arya, "Performance analysis of artificial bee colony optimization based clustering protocol in various scenarios of WSN", Procedia Computer Science, Volume 132, 2018, Pages 183-188, ISSN 1877-0509,
[36] Yinggao Yue, Jianqing Li, Hehong Fan, Qin Qin, "Optimization-Based Artificial Bee Colony Algorithm for Data Collection in Large-Scale Mobile Wireless Sensor Networks", Journal of Sensors, vol. 2016, Article ID 7057490, 12 pages, 2016.
[37] Y. Pinar, A. Zuhair, A. Hamad, A. Resit, K. Shiva and A. Omar, "Wireless Sensor Networks (WSNs)," 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT), 2016, pp. 1-8, doi: 10.1109/LISAT.2016.7494144.
[38] S. Srivastava, M. Singh and S. Gupta, "Wireless Sensor Network: A Survey," 2018 International Conference on Automation and Computational Engineering (ICACE), 2018, pp. 159-163.
[39] Mohammed Sulaiman BenSaleh, Raoudha Saida, Yessine Hadj Kacem, Mohamed Abid, "Wireless Sensor Network Design Methodologies: A Survey", Journal of Sensors, vol. 2020, Article ID 9592836, 13 pages, 2020.
[40] Rehman, Au., Rehman, S.U. & Raheem, H. Sinkhole Attacks in Wireless Sensor Networks: A Survey. Wireless Pers Commun 106, 2291–2313 (2019).
[41] H. Shafiei, A. Khonsari, H. Derakhshi, P. Mousavi, Detection and mitigation of sinkhole attacks in wireless sensor networks, Journal of Computer and System Sciences, Volume 80, Issue 3, 2014, Pages 644-653, ISSN 0022-0000,
[42] P. Reindl, K. Nygard and X. Du, "Defending Malicious Collision Attacks in Wireless Sensor Networks," 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, 2010, pp. 771-776.
[43] H. Shafiei, A. Khonsari, H. Derakhshi, P. Mousavi, “Detection and mitigation of sinkhole attacks in wireless sensor networks”, Journal of Computer and System Sciences, Volume 80, Issue 3, 2014, Pages 644-653, ISSN 0022-0000,
[44] Tejinderdeep Singh and Harpreet Kaur Arora, “Detection and Correction of Sinkhole Attack with Novel Method in WSN Using NS2 Tool” International Journal of Advanced Computer Science and Applications(IJACSA), 4(2), (2013).
[45] Puneet Azad, Vidushi Sharma, "Cluster Head Selection in Wireless Sensor Networks under Fuzzy Environment", International Scholarly Research Notices, vol. 2013, Article ID 909086, 8 pages, 2013.
[46] Amin Shahraki, Amir Taherkordi, Frank Eliassen, "Clustering objectives in wireless sensor networks: A survey and research direction analysis", Computer Networks, Volume 180, 2020,107376, ISSN 1389-1286,
[47] Rupinder Singh, Jatinder Singh, Ravinder Singh, "Fuzzy Based Advanced Hybrid Intrusion Detection System to Detect Malicious Nodes in Wireless Sensor Networks", Wireless Communications and Mobile Computing, vol. 2017, Article ID 3548607, 14 pages, 2017.
[48] Tiwari, Virendra., Waoo, A. ,A. , "Comprehensive Study on Metaheuristics FADEBased Artificial Bee Colony Optimization Algorithm to Improve Performance of Wireless Networks", International Journal of Scientific Research in Computer Science, Engineering and

InformationTechnology (IJSRCSEIT), ISSN: 2456-3307, Volume6 Issue 5, pp. 236-243, September-October 2020.

[49] Sibi Amaran, Dr. R. Madhan Mohan, "Differential Evolution with Artificial Bee Colony Optimization Algorithm based Sink Hole Detection in Wireless Sensor Networks", IJETER, Volume 8. No. 5, May 2020.

[50] Syed, M. and Dubey, M., "A Novel Adaptive Neuro-fuzzy Inference System-Differential Evolution (Anfis-DE) Assisted Software Fault-tolerance Methodology in Wireless Sensor Network (WSN)," 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), (2019).