Hybrid Ant Colony Optimization for Sinkhole Detection in WSN

Madhu Nagaraj[1], Rampur Srinath[2]

[1]PG Student, Dept. of Information Science and Engineering, NIE, Mysore, India
[2]Associate Professor, Dept. of Information Science and Engineering, NIE, Mysore, India

Abstract - *In a Wireless Sensor Network (WSN), grouping is among the most important tasks, in which one of the hubs from a group of hubs is chosen to be the group head, as well as the group head is liable for both standard activities and the administration of other hubs within the group. Malicious hub finding is also essential in the wireless sensor network (WSN), with the purpose of preventing the malicious hub from becoming the group head. Furthermore, as the malicious hubs grow, so does the likelihood of becoming a malicious hub as a bunch head increases. A Hybrid Ant Colony based pernicious hub location and bunch head choosing approach is presented to identify harmful hub as well as to choose a relatively high hub for the center point. The suggested calculation identifies sinkhole detection for malicious hubs, after which a high-potential hub is chosen as the bunch head. This approach also reduces bunch covering with group head geographical distribution, much as removing spiteful hubs expressly does not allow malevolent hubs to become bunch heads, resulting in an overall increase in energy effectiveness.*

Key Words: **Hybrid Ant Colony, clustering, fuzzy, WSN**

1. INTRODUCTION

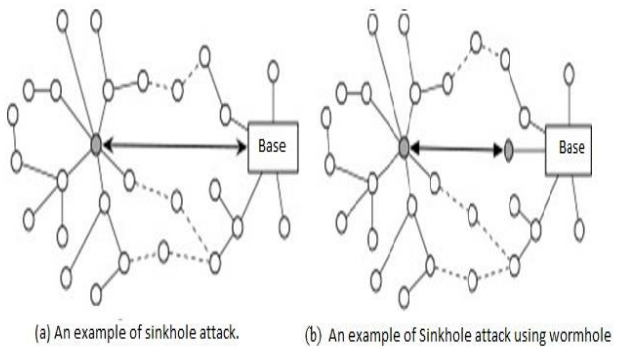
A wireless sensor network (WSN) is made up of a collection of sensor hubs that work together in a group to complete a specific task (for example, environmental variables management, target follow-up, and so on) and then send the gathered data to a base station or controller via a distant medium. WSN is defined as a collection of cooperating hubs with detecting, reasoning, and remote correspondence capacities. The sensor hubs combine and transfer data to the detached base station, from which the end client can obtain the required information [8]. The sensed data is also collected 'inside the company' at sink hubs, which may be sensors or different hubs fortunate to be in potential merely as assets. The information is then periodically and on-request delivered to the end customers via the sinks or a higher request hub the base station [9]. Wireless sensor networks are used for a variety of purposes, including common, medical, and environmental services, as well as military applications. Target tracking in combat, territorial administration, common work monitoring, environmental issues oversight, and plant maintenance are only a few examples of many types of applications. Due to the functioning of a large number of sensor hubs in inclement weather, certain nefarious hubs may infiltrate the organization, causing routine operations to be hampered. And reduced energy proficiency [13] can also have an impact on group preparation.

2. SINKHOLE ATTACK

WSNs are vulnerable to a variety of risks, including sinkhole attacks, which have been regarded as one of the most significant. A rogue node advertises itself as the best possible path to the base station in this form of attack, deceiving its neighbors into using the route more frequently. As a result, the malicious node has the ability to tamper with data, disrupt normal operations, and even pose a number of other threats to the network's security.

Sinkhole assaults can be carried out by one of two sorts of attackers: malicious insider and resourceful outsiders. In the first scenario, an adversary uses a compromised node to start a deception attack by promoting a route to neighbors. In the latter situation, a laptop-class adversary with high-performance computing and communication skills establishes a single-hop route from its surrounding region to the base-station, persuading the neighbors to send all traffic through it. Furthermore, the high-quality route draws not only the sinkhole's neighbors, but practically all nodes that are closer to the sinkhole than the base-station (perhaps from several hops away), amplifying the hazard. A sinkhole attack is depicted in Figure 1(a).

Wormhole attack can also be used to create a sinkhole. In this form of attack, a malicious node steals a routing packet from one of its neighbors and sends it to another colluding node over a secret tunnel. The message is eventually delivered to the base station by the colluding node. Despite the fact that the tunnel's two ends are separated by a greater distance than other routes, it can prevent the source from identifying other lawful routes that are more than two hops away from the destination, disrupting network functionality. An example of such an attack is shown in Figure 1(b).



(a) An example of sinkhole attack. (b) An example of Sinkhole attack using wormhole

Fig-1: Different types of sinkhole attacks.

3. RELATED WORK

Inside and outside prologue to WSNs, as well as their properties, have been specified in[1]. Several ways for extending the lifetime of an organization have been proposed in recent years, one of which is selecting a group leader based on distance [2]. Several methods discovered in the writing study revolve around spiteful hub discovery and anticipation, such as in [3], where sinkhole effects on network borders are assessed, as well as tactics for avoiding and locating sinkhole assault in WSN In [4], a process for detecting spiteful hubs was discussed in light of the excellent trust strategy. Previously, other computational methods-based group-determination methodologies have been presented, such as the Cluster Head Choice Convention (CHFL) [10]. Cluster Head Election Instrument (CHEF) [11] methodology used a similar concept of utilizing Fuzzy Logic. Finally, the capability of hubs bunches of work has been determined, for example, using the ACE calculation [12], which evaluates each hub's potential individually for each bunch head choice.

In order to deal with WSN concerns, a variety of knowledge calculations have been used (Kulkarni and Venayagamoorthy, 2011; Zungeru et al., 2012; Saleem et al., 2011). ACO is one of a slew of new insights spurred by the scavenging behavior of insects that collaborate to find the shortest path between home and food source (Singh et al., 2010). It is based on the concept of synthetic compounds known as pheromones, which are used to accomplish hub selection through circuitous correspondences between insects (Lee et al., 2011). Multitude knowledge is a subcategory of artificial intelligence inspired by the shrewd behavior of social insects such as honey bees, subterranean insects, wasps, and termite's in common biological frameworks (Jangra et al., 2013). The fake honey bee state calculation, which is based on the searching behavior of bumble bees, and the molecule swarm knowledge, which is based on the behavior of bird running and fish tutoring, is two examples of multitude insight (Zhao et al., 2010).

The ACO calculation was used in WSN because it can easily be altered to deal with both static (Acharya et al., 2009; Singh and Behal, 2013) and dynamic (Zhong and Zhang, 2012; Ye and Mohamadian, 2014) combinatorial improvement problems. ACO can be used to solve a variety of problems, including directing and load regulating. In terms of direction, the ACO computation is frequently employed in a metaheuristics method to determine the best paths from source to objective. In addition to determining appropriate courses, the stagnation problem, in which a significant number of parcels are consigned to the same sensor hub, resulting in the hub having a high level of responsibility, can be addressed in the long run using the heap adjusting technique. This is due to the fact that by applying both global and local pheromone updates, the best paths may vary from time to time. In any case, the ACO's display is a must-see, Calculations may also be used to achieve the highest throughput, the least deferral, the least energy use of sensor hubs, the least stagnation issue, and to alter the entire sensor hubs while simultaneously extending the WSN organization's lifetime.

4. PROPOSED ALGORITHM

Hybrid Ant Colony BASED SINKHOLE NODE DETECTION AND CLUSTERING (HYBRID ANT COLONY-NMDC). Hybrid Ant Colony-NMDC works in four stages.

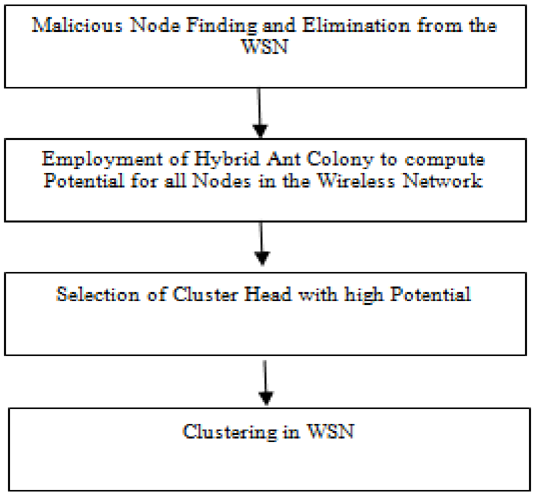

Malicious Node Finding and Elimination from the WSN
Employment of Hybrid Ant Colony to compute Potential for all Nodes in the Wireless Network
Selection of Cluster Head with high Potential
Clustering in WSN

Fig-2: Hybrid Ant Colony-NMDC Stages

Malicious Node finding and Elimination

The noxious hub discovering calculation is used in this paper, which is based on trust highlight. Fig 3 shows the formula for malicious hub recognition based on trust. All malicious hubs that have been identified are then deleted, such as when choosing the bunch head.

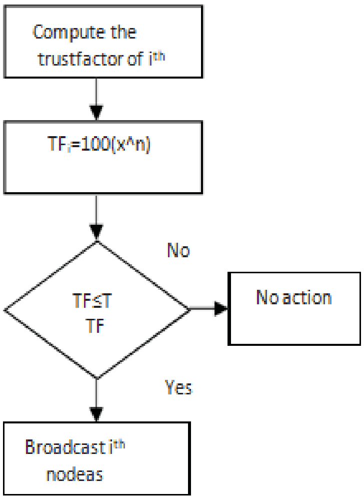

Compute the trustfactor of i^{th}
TF_i=100(x^n)
TF≤T TF
No
No action
Yes
Broadcast i^{th} nodeas

Fig-3: Malicious node detection

Employment of Hybrid Ant Colony to find the potential of each node

Using Hybrid Ant Colony, the capability of each hub in the organization is discovered at this stage. Hybrid Ant Colony has two known conditions [5-6].

$$V_i = v_i + rand * (P_{besti} - S_i) + rand * (g_{best} - S_i)$$ □□□

$$S^{k+1} = S^k + V^{k+1}$$ □□□

The capability of each hub in the organization is determined by using a Hybrid Ant Colony with fluffy logic and three information boundaries, such as the hub's remaining energy, supported inclusion, and connection quality.

Remaining energy: Applying the following condition, the excess energy (REi) of each hub (Ni) arising from one information transmission is determined:

$$RE_i = IE - (TE + RE)$$ □□□

Where IE is the hub's initial energy, and TE and RE are the energies consumed when the transmission and collection of data is completed. Sponsored inclusion is the process of identifying the location of a hub encased by its neighboring hub as part of an area established district. If two hubs X and Y are separated by a distance d, the supported inclusion of Y for X can be found through the focal point 2, which may be calculated according to the following condition:

$Cos\ \sigma$ □ $d^2 + X^2 - Y^2/2Xd$ □□□

Link quality: It depicts the presentation of strength as well as the nature of an obtained bundle. It certainly depends on the signal strength obtained (RSSI). LQ's value ranges from 0 to 255.

LQ ˥ $RSSI$ □□□

RSSI is now defined as the ratio of the received power (Prx) to the reference power (Pr). Pr is nearly identical to outright esteem, i.e. 1 mW, in most cases.

$RSSI = 10.Log\ (P_{rx}/\ P_{ref})$ dbm □□□

As Prx rises, so does RSSI, which aids link quality [7]. So, as previously stated, these three boundaries are involved in the evaluation of each hub's capability. In this paper, Mamdani's technique in the derivation cycle was used because it is more commonly used in applications. Fluffy reasoning with Hybrid Ant Colony is deployed in the NS2 test system in this research to examine the organization's execution with three information boundaries. The organization test system is given boundaries of the recreation as a result of the execution of these means. The log records are next provided to the log analyzer, where the upsides of goal capacities are once again provided to the fluffy surmising motor of Hybrid Ant Colony-NMDC, as a result of rebuilding the code. The flowchart for Hybrid Ant Colony-NMDC is shown in Figure 4.

Cluster Head Selection

Regardless, group chiefs are chosen from 7 to 9% of the hubs (Pinitial) with the highest potential. After then, all of the leftover hubs with the most potential are considered, and their distance D from the complete bunch of heads is calculated. The base distance Dmin and the limit distance Dthreshhold are currently used as criteria for selecting the group leader. Dthreshhold is the minimum distance required to maintain contact between two group chiefs. If Dmin is greater than Dthreshhold, the hub is chosen to be the group's leader. Another issue is that if Dmin is not equal to Dthreshhold, the hub is discarded, for example, no group leader is chosen, and this is done to avoid bunch covering.

Clustering

We did bunching in this work according to the CFHL [10] standard, which is the most well-known in the remote sensor organization. In this grouping strategy, the chosen bunch heads transmit a message to all hubs in their transmission range, and once the message has been received by the Non-bunch head, it can choose the source of the most extreme sign force as their bunch head. If there is a tie, the group leader with the smallest hub's ID is chosen.

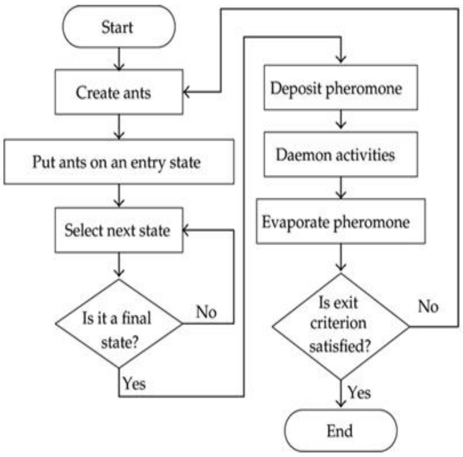


Fig-4: Description of Hybrid Ant Colony-NMDC Algorithm

5. ADVANTAGES AND DISADVANTAGES OF ANT COLONY OPTIMIZATION IN WSN

In WSN, the ACO is typically used to increase directing, energy production, energy usage, and deferral. This is the result of ACO conduct, which can provide an optimum steering path from the source hub to the objective hub, improving energy efficiency, energy consumption, and reducing delay. The ACO computation is adaptable to static, dynamic, and variable situations (Camilo et al., 2006). In a static WSN environment, the source hub and objective hub are always in the same place, however in a portable WSN environment, underground insects collaborate to find the shortest path between home and food supply (Singh et al., 2010). It works on the basis of synthetic compounds known as pheromones, which are used to perform backhanded correspondences amongst underground bugs (Lee et al., 2011). Multitude insight is a type of artificial reasoning inspired by the intelligent behaviour of social insects such as honey bees, insects, wasps, and termites in natural settings (Jangra et al., 2013). The counterfeit honey bee settlement calculation, which is based on the rummaging behaviour of bumble bees, and the molecular swarm insight, which is based on the behavior of bird rushing and fish tutoring, are two examples of multiplicity knowledge (Zhao et al., 2010).

Because the ACO computation is effective in resolving both static (Acharya et al., 2009; Singh and Behal, 2013) and dynamic (Zhong and Zhang, 2012; Ye and Mohamadian, 2014) combinatorial enhancement concerns, it has been used in WSN. ACO can be used to solve a variety of problems, including directing and load regulating. In terms of steering, the ACO computation is frequently employed in a metaheuristics method to determine the best paths from source to objective. The issue of stagnation, when a large number of bundles are assigned to the same sensor hub, resulting in the hub having a high responsibility, can be solved using the heap adjustment technique, in addition to choosing appropriate courses. This is because the best pathways may alter from time to time as a result of global or possibly nearby pheromone refreshes. However, the display of the ACO calculation can be extended to get the highest throughput, the least delay, the least energy use of sensor hubs, the least stagnation issue, to change all sensor hubs at the same time, and to extend the WSN's organization lifetime.

6. PERFORMANCE ANALYSIS

Hybrid Ant Colony-NMDC set forward group heads in a spatially circulated way while also developing extra bunches to comply with hubs along the entire path in the organization, as seen in the reproduction. The advantage of spatially scattered bunches is that it regulates the energy consumption of hubs in WSNs. Hybrid Ant Colony-NMDC also eliminates malicious hubs, resulting in less bundle misery as proven by majority throughput, indicating that the absolute surplus energy of hubs in Hybrid Ant Colony-NMDC is superior to CHFL as a differentiator. As illustrated, Hybrid Ant Colony-NMDC provides an all-encompassing organization with its hubs present in the organization for a longer period of time than CHFL.

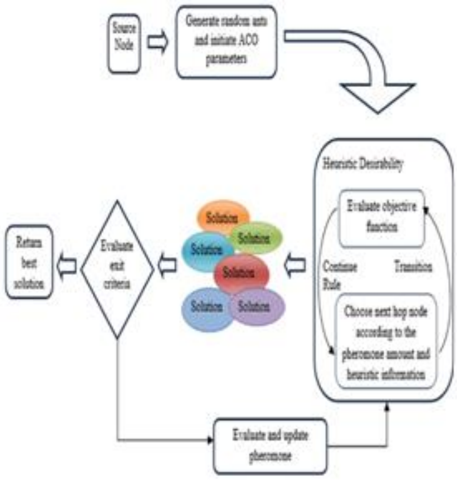
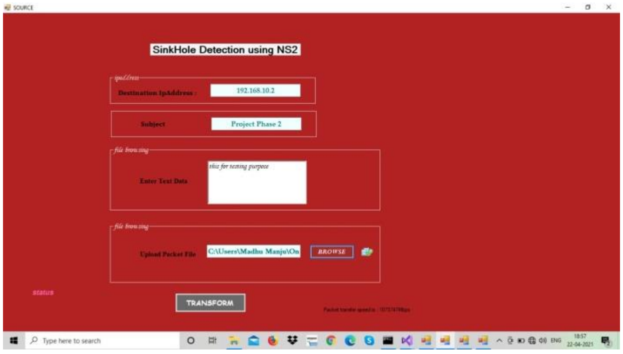

Source Node
Generate random ants and initiate ACO parameters
Heuristic Desirability
Evaluate objective function
Continue Rule
Transition
Choose next hop node according to the pheromone amount and heuristic information
Solution
Solution
Solution
Solution
Solution
Solution
Evaluate exit criteria
Return best solution
Evaluate and update pheromone

Fig-5: Ant colony optimization



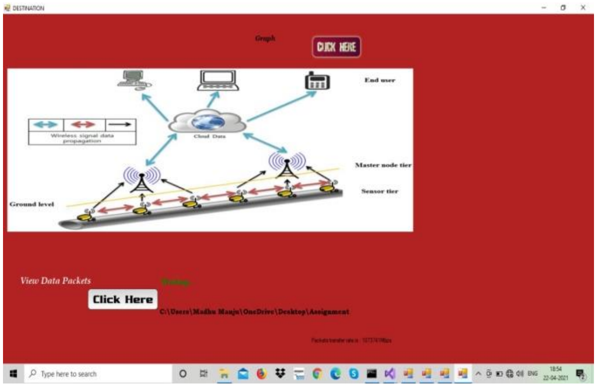
Destination IpAddress : 192.168.10.2

Subject Project Phase 2

Enter Text Data this for testing purpose

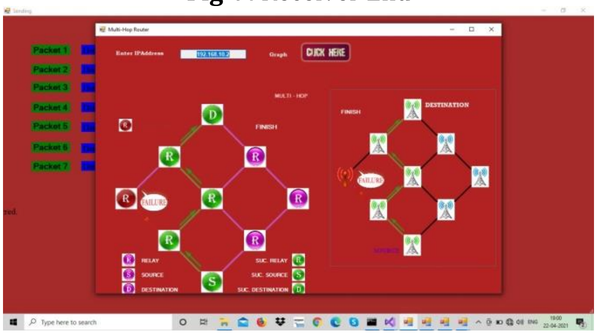
Upload Packet File C:\Users\Madhu Manju\On

Fig-6: Sender End



C:\Users\Madhu Manju\OneDrive\Desktop\Assignment

Fig-7: Receiver End



Enter IPAddress 192.168.10.2

Fig-8: Packets Transmission Structure

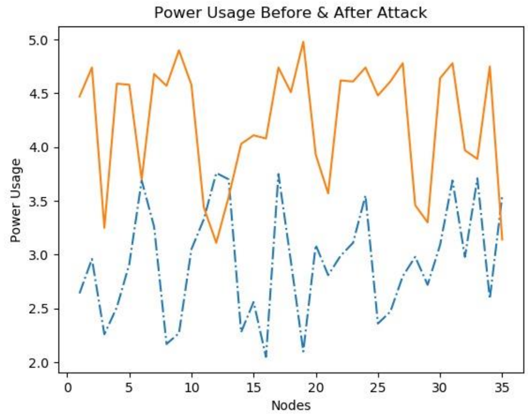


Fig-9: Comparative study graph for sinkhole attack

Table -1: Summary of the Parameters Used In Simulations

Parameter	Value
T_X Power	0.670
R_X Power	0.400
Rate	250 kb
Simulation time	100 s
MAC	802.11
Antenna	Omni antenna
Area	500x500
Initial energy	10.1 J

Table -2: Simulation Results

Simulation Results	Hybrid-NMDC	CHFL
Percentage of cluster head	6%	13%
Number of cluster heads	15	16
Number of malicious nodes	12	12
Number of cluster	11	10

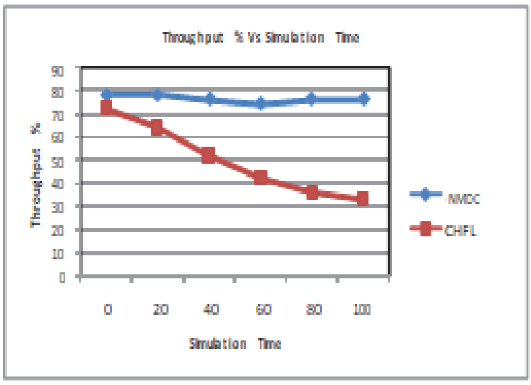


Fig- 10: Throughput vs. simulation time

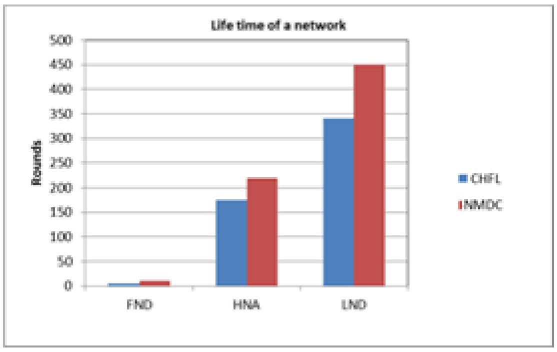


Fig-11: Life time of network.

7. CONCLUSION

To extend the lifetime of the network as well as to provide reliable and efficient communication in a distant sensor network, the protocol used must be energy efficient, which can be achieved by employing a high-quality grouping technique. A Hybrid Ant Colony-based approach for sinkhole detection and picking a bunch head in a remote sensor network is proposed in this research. The suggested computation is based on three information limits, such as the hub's remaining energy, supported inclusion, and connection quality, which determine each hub's capabilities in the WSN. Hybrid Ant Colony these three information boundaries are used to register the competence of each hub. The grouping calculation (Hybrid Ant Colony-NMDC) suggested in this study uses a regionally distributed approach for picking bunch heads, which reduces group coverage while increasing energy efficiency. Hybrid Ant Colony-NMDC recognizes vengeful hubs and does not allow them to be the group leader; this means Hybrid Ant Colony-NMDC expands dependability and creates sensor networks as deficiency tolerant organizations. In this way, Hybrid Ant Colony-NMDC overcomes CHFL's present flaws, such as bunch covering and overhead. With these qualities, the proposed calculation Hybrid Ant Colony-NMDC confirms to be the unequalled option where less energy consumption is desired as well as an increase in network lifetime.

REFERENCES

[1] Bhawnesh Kumar, Vinit Kumar Sharma, Distance based Cluster Head Selection Algorithm for Wireless Sensor Network. International Journal of Computer Applications (0975 – 8887) Volume 57– No.9, November 2012.

[2] Mohammad Wazid, Avita Katal, Roshan Singh, Sachan, R H Goudar, D P Singh, Detection and Prevention Mechanism for Blackhole Attack in Wireless Sensor Network. International conference on Communication and Signal Processing, April 3- 5, 2013.

[3] Yuanpeng Xie, Jinsong Zhang, Ge Fu, Hong Wen, Qiyi Han, Xiping Zhu, Yixin Jiang, Xiaobin Guo, The Security Issue of WSNs Based on Cloud Computing. IEEE Conference on Communications and Network Security 2013 - Poster Session.

[4] Sachin Gajjar, Mohanchur Sarkar, Kankar Dasgupta, Cluster Head Selection Protocol using Fuzzy Logic for Wireless Sensor Networks. International Journal of Computer Applications (0975 – 8887) Volume 97– No.7, July 2014.

[5] Shabana Mehfuz, Sumit Kumar "Two dimensional particle swarm optimization algorithm for load flow analysis" International Journal of Computational Intelligence Systems, Vol. 7, Iss. 6, pp. 1074-1082, Sept 2014.

[6] Bagheri, T.: 'DFMC: decentralized fault management mechanism for cluster based wireless sensor networks'. Second Int. Conf. on IEEE Digital Information and Communication Technology and its Applications (DICTAP), 2012, 2012, pp. 67--71.

[7] Sumit Kumar, Shabana Mehfuz, "Efficient Fuzzy Logic Based Probabilistic broadcasting for mobile ad hoc network", International Journal of Computational Intelligence Systems, Vol. 9, No. 4, pp. 666-675, June 2016.

[8] Shabana Mehfuz , Sumit Kumar "Energy Aware Probabilistic Broadcasting for Mobile Ad Hoc Network" in 2nd IEEE International Conference on Computing for Sustainable Global Development,2015,pp 1028 - 1033

[9] Sumit Kumar, Shabana Mehfuz "Energy Efficient Probabilistic broadcasting for mobile ad hoc network" Journal of the Institution of engineers (India): Series B, Volume 98, Issue 3, pp 289–294, June 2017.

[10] J. M. Kim, S. H. Park, Y. J. Han, and T. M. Chung, "CHEF: cluster head election mechanism using fuzzy logic in wireless sensor networks", Proc. of International Conference on Advanced Communication Technology, pp.654–659, 2008.

[11] Chan H. and Perrig A. "ACE: An Emergent Algorithm for Highly Uniform Cluster Formation", Proc. of 1st European Workshop on Sensor Networks, pp. 154–171, 2004.

[12] Sumit Kumar, Shabana Mehfuz, "Intelligent probabilistic broadcasting in mobile ad hoc network: A Hybrid Ant Colony approach", Vol.2, Issue 2, pp. 107-115, July 2016.

[13] Raghavendra V. Kulkarni, Anna Forster, and Ganesh Kumar Venayagamoorthy, "Computational Intelligence in Wireless Sensor Networks: A Survey," IEEE Communications Surveys and Tutorials, vol. 13, no. 1, pp.68- 96, 2011.

[14] Kala, P.C., Agrawal, A.P. and Sharma, R.R., 2020, January. "A Novel Approach for Isolation of Sinkhole Attack in Wireless Sensor Networks". In 2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence) (pp. 163-166). IEEE.

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

[16] Nwankwo, K. E. (2019, October). Sinkhole Attack Detection in A Wireless Sensor Networks using Enhanced Ant Colony Optimization to Improve Detection Rate. In 2019 2nd International Conference of the IEEE Nigeria Computer Chapter (NigeriaComputConf) (pp. 1-6). IEEE.

[17] Kesav Unnithan, S.L., Lakshmi Devi, C. and Sreekuttan Unnithan, C., 2015. "Survey of Detection of Sinkhole Attack in Wireless Sensor Network". International Journal of Computer Science and Information Technologies (IJCSIT), 6(6), pp.4904- 4909.