Energy Consumption Minimization using GWO Tuned based Fuzzy Logic

Kanika Madaan, Bindu Rani, Ravi Malik
Student, Student, Assistant Professor (HOD)
Electronics & Communication Engineering Department
Geeta Engineering College, Panipat, India.

Abstract- The popularity of Wireless Sensor Networks (WSN) has increased rapidly and tremendously due to the vast potential of the sensor networks to connect the physical world with the virtual world. Since sensor devices rely on battery power and node energy and may be placed in hostile environments, so replacing them becomes a difficult task. Thus, improving the energy of these networks i.e. network lifetime becomes important. The thesis provides methods for clustering and cluster head selection to WSN to improve energy efficiency using a fuzzy logic controller. It presents a comparison between the different methods on the basis of the network lifetime. It compares existing ABC optimization method with the Gray wolf optimization (GWO) algorithm for different size of networks and different scenario. It provides cluster head selection method with good performance and reduced computational complexity. In addition, it also proposes GWO as an algorithm for clustering of WSN which would result in improved performance with faster convergence.

***Keywords*- MANET, WSN, GWO, Fuzzy logic etc.**

I. INTRODUCTION

A Wireless sensor network can be defined as a network of devices that can communicate the information gathered from a monitored field through wireless links. The data is forwarded through multiple nodes, and with a gateway, the data is connected to other networks like wireless Ethernet.

Some factor is in mind while design a sensor network. The energy consumption should be very less. The sensor networks are unique because they are easily implemented in to the communication links and channels. Some nodes and sink are provided in the network. The sink node(s) are very important terms in case of WSN. Thus, communication in sensor networks is typically referred to as data-centric, rather than address-centric, and data may be aggregated locally rather than having all raw data sent to the sink(s). These unique features of sensor networks have implications in the network layer and thus require a re-thinking of protocols for data routing. In addition, sensors often have knowledge of their own location in order to meaningfully assess their data. This location information can be utilized in the network layer for routing purposes. Finally, if a sensor network is well connected (i.e., better than is required to provide communication paths), topology control services should be used in conjunction with the normal routing protocols.

Clustering for Data Aggregation

For designing a sensor network we required large number of node, protocol scalability. If the sensors are managed directly by the base station, communication overhead, management delay, and management complexity become limiting factors in network performance.

Clustering has been proposed by researchers to group a number of sensors, usually within a geographic neighborhood, to form a cluster that is managed by a cluster head.

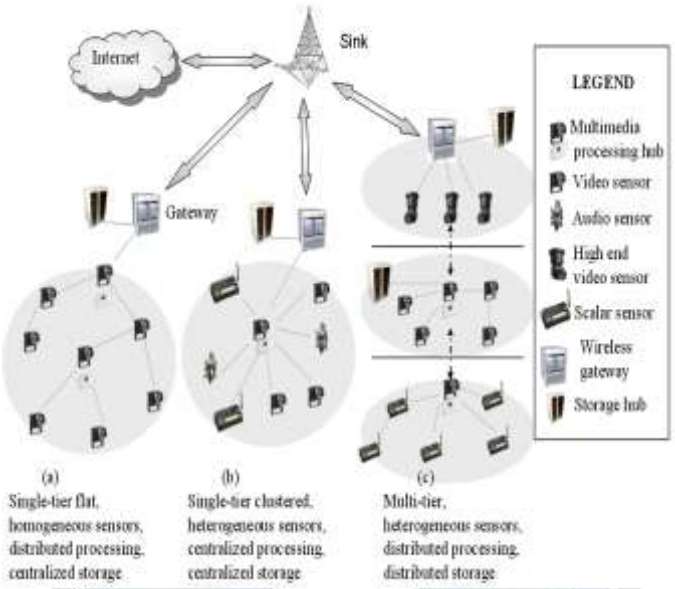

Figure 1: Wireless sensor networking [2]

.

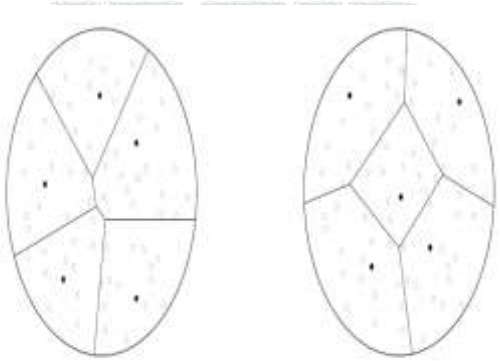

Figure 2: Adaptive clustering of the network [2].

II. ATTACKS IN WSN

Table1: various attacks in different layers

Layer	Attacks
Physical layer	Jamming, Tampering, Sybil Attack
Data Link Layer	Collision, Sybil Attack, Spoofing and Altering Routing Attack, Replay attack
Network Layer	Internet smart attack, Sybil Attack, Black hole Attack, Spoofing and Altering Routing Attack, wormhole attack, selective forwarding attack, Hello Flood Attack, sink Hole Attack
Transport Layer	Flooding Attack, De synchronization
Application	Spoofing and Altering Routing Attack, False Data Injection

Denial of Service (DoS) attacks: This attack is an explicit attempt to prevent the legitimate user of a service or data. The common method of attack involves overloading the target system with requests, such that it cannot respond to normal traffic. As a result, it makes the system or service unavailable for the user. The basic types of attacks are: Jamming, Tapering, Collision, Homing and Flooding. If a sensor network encounters DoS attacks, the attack gradually reduces the functionality as well as the overall performance of the wireless sensor network. In WSNs several types of DoS can be performed in different layers which are tabulated in Table 2

Table 2: Layer Based DOS Attacks

Layer	Attacks
Physical layer	Jamming, Tampering
Data Link Layer	Collision, Exhaustion
Network Layer	Misdirection
Transport Layer	De synchronization
Application	Path Based DOS

III. PROPOSED WORK

The main steps of our work can be summarized as follows:

- An optimized Sugeno fuzzy inference system (FIS) is proposed as an efficient and fast, application specific routing protocol in Wireless Sensor Network environment. We have designed three membership function with 27 set of rules in Sugeno K-means algorithm is utilized to form balanced clusters over the network.
- An objective function is made to calculate residual energy (RE), distance of node from sink (DNS), distance of node from centroid (DNC). Position of centroid is calculated by K-means algorithm. Objective function also find position of Cluster Head on the basis of fuzzy inference system.
- Grey Wolf Optimization (GWO) algorithm is implemented to optimize the fuzzy rules of FIS file in order to prolong the network lifetime, based on the different application specifications. Flow chart of our work is given below for easy understanding.

As the fuzzy inference system FIS can achieve a better combination of the all input parameters to obtain the optimal output. So a Sugeno FIS is constructed in MATLAB. The fuzzy controller consists of three parts: first is fuzzification in which real environment variables are converted to fuzzy variables, second is inference model which inherits the rule sets or decision variables and third is defuzzification which reverse the fuzzy variables to environment variables. The fuzzy logic controller for the case has three real time inputs measured by objective function for each node in a cluster. These are:

- Residual energy of node (RE)
- Distance of node from sink of cluster (DNS)s
- Distance of node from centroid of cluster

A typical Sugeno fuzzy rule with three inputs *x, y* and *z*, (RE, DNS, DNC) and one output *w* can be shown as

$$IF = p \times x + q \times y + r \times z$$

Where p, q, r, are weight age of three variables, RE, DNS, DNC. We considered there values as 0.5, 0.3, 0.2 in the order of priorities. Normalization function used to normalize input variable with in required range is given below.

$$Normalized\ x_i = \frac{x_i - \min(x)}{\max(x) - \min(x)}$$

Membership functions for input to FIS is designed by taking some assumptions. These are:

1. Limits of RE input after normalization is 0 to1
2. Limits of DNS and DNC input is -1 to 0
3. Trapezoidal membership functions are used for each input
4. Initial values of range for Low membership input considered 0-0.1, for Medium membership input considered .026-0.65 and for High membership input considered 0.66-1, for RE input.
5. Initial values of range for Low membership input considered -0.25 to 0, for Medium membership input considered -0.64 to -0.25 and for High membership input considered -1 to -0.65, for DNS input.
6. Initial values of range for Low membership input considered -0.25 to 0, for Medium membership input considered -0.64 to -0.25 and for High membership input considered -1 to -0.65, for DNC input.

The surface viewer of our fuzzy logic is shown in figure 3 . It is a three-dimensional representation of mapping of error and output of fuzzy logic.
This decision will depend on the input values for the system. The defuzzified output is displayed as a bold vertical line on this plot. The Rule Viewer allows you to interpret the entire fuzzy inference process at once.

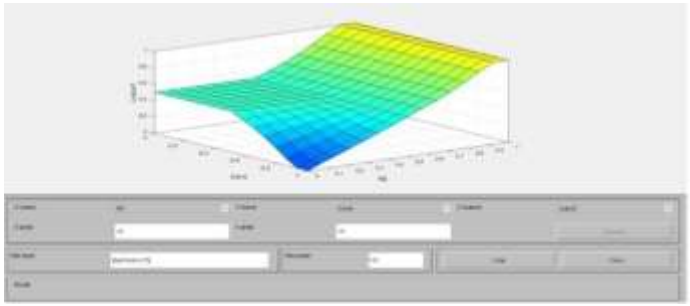

Figure 3: Surface viewer plot of fuzzy logic

.

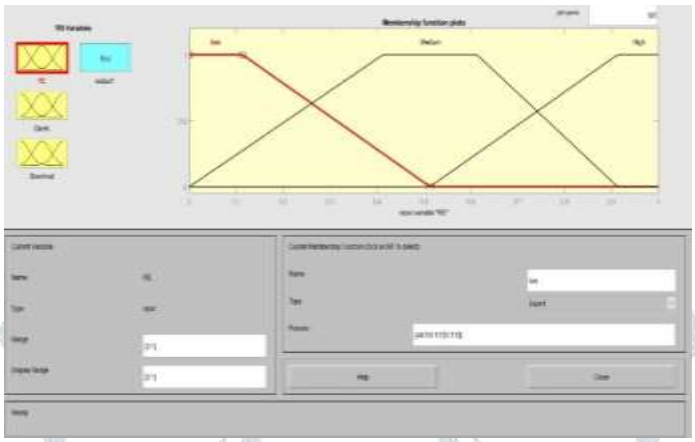

Figure 4: Membership function of input RE

Algorithm Steps

A step by step algorithm for the proposed work is given as:

STEP1. Initialize the node population random positions and directions of bacteria.

STEP2. Apply K-means clustering technique to make clusters of nodes and their centroids.

STEP3. Create an objective function which can calculate RE, DNS. DNC and also choose CH on the basis of RE and calculates mean RE of clusters and total node population.

STEP4. Create a Fuzzy Inference System FIS using Sugeno function for three inputs RE,DNS,DNC and make their membership function and rule set to decide output.

STEP5. Initialize random positions of grey wolves within the search space limits.

STEP6. Consider the searching space dimension as number of membership function values to be tuned which is 15 in our case.

STEP7. For each randomly generated set of membership functions, calculate the objective function as in equation 16.

STEP8. Compare the mean of residual energy in each cluster for each wolf and consider the best position till now which is having maximum residual energy.

STEP9. Take three best wolves positions and update them as

X1=Alpha_pos(j)-A1*D_alpha;
X2=Beta_pos(j)-A2*D_beta;
X3=Delta_pos(j)-A3*D_delta

STEP10. The mean of these three best wolves' positions is taken as the updated positions and objective function is calculated again for new membership functions.

STEP11. The best value received by this step is compared with the best positions' value in step8 and maximum of those is the best membership functions till now.

STEP12. This process is repeated till all iterations are not exhausted.

STEP13. The best result obtained after all iterations is considered as the convergence point and used as the final fuzzy logic membership functions range.

IV. RESULTS AND DISCUSSION

Case-1 When Geographical area is 50mx50m

When geographical area is 50 m^2 then we calculated and observed imapct of GWO and ABC algorithm on increasing the lifetime of WSN.

Here are results of this case:

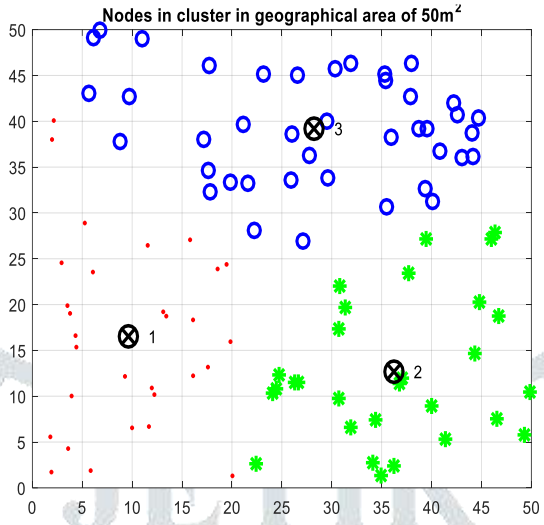

Figure 5 Nodes in cluster in geographical area of 50 m^2

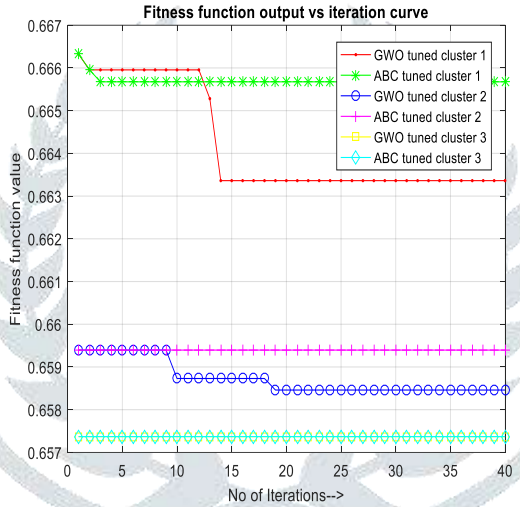

Figure 6 COnvergence Curve for the GWO and ABC comaprsion for cluster head selection in WSN

We used grey wolf optimization algorithm to optimally select the cluster head which has the maximum residual energy. The optimisation algorithm is said effective only when it decreases with iterations and settle after few iterations. As soon as it settles, good ios the optimization. In our case we have considered the objective function which is calculating the residual energy and finally takes inverse of mean of residual energy so that the GWO algorithm can work to minimize. A convergence curve fo GWO for three clusters cases is shwon in figure 7 In it the graph decreases with iterations and saturates after certain iterations. The convergence results are compared with ABC algorithm too.

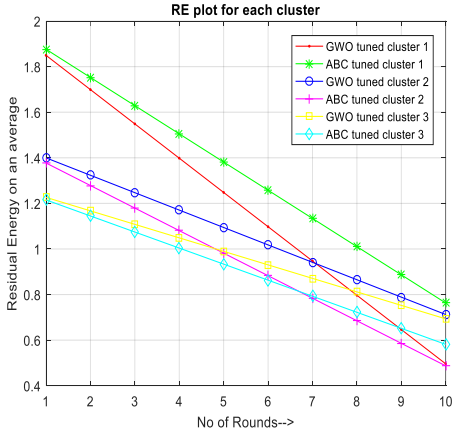

Figure 7 RE plot of GWO and ABC

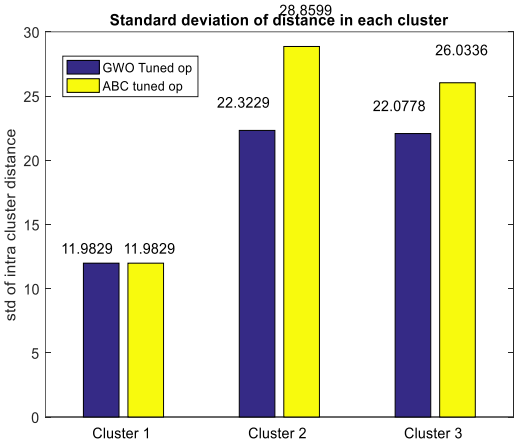

Figure 8 Standard deviation of cluster distance

Table 3 Cluster-wise comparsion for GWO and ABC for case-1 for standard deviation of distance in clusters

Case-1 50m^2	**Cluster 1**	**Cluster 2**	**Cluster 3**
GWO	11.98	22.3229	22.07
ABC	11.98	28.85	26.03

Case-2 When Geographical area is 100mx100m

When geographical area is 100 m^2 then we calculated and observed imapct of GWO and ABC algorithm on increasing the lifetime of WSN.

Here are results of this case:

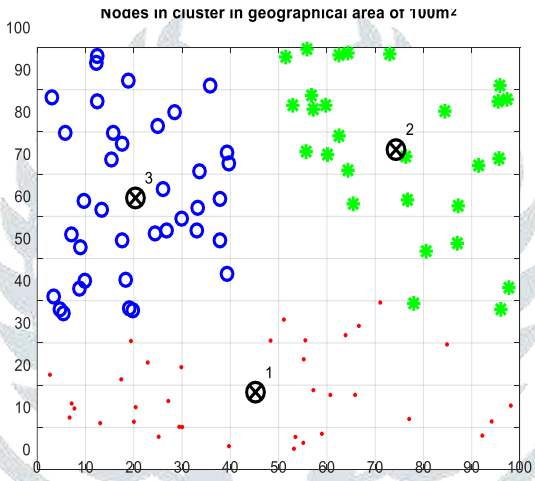

Figure 9 Nodes in cluster in geographical area of 100 m^2

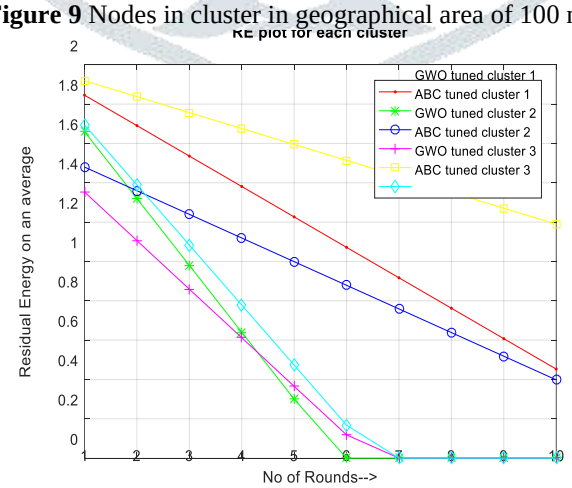

Figure 10 RE plot of GWO and ABC

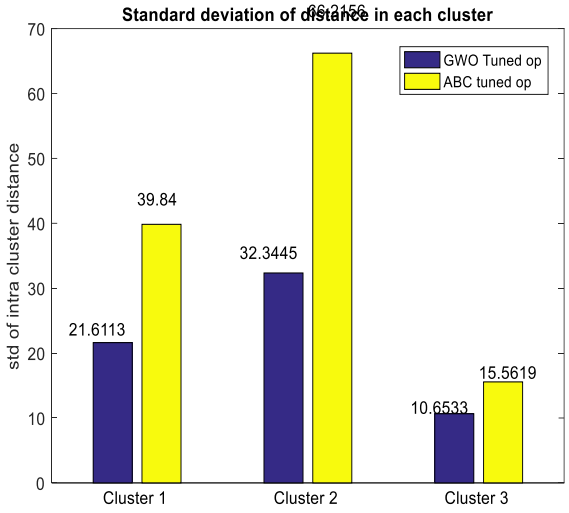

Figure 11 Standard deviation of cluster distance

Table 4 Cluster-wise comparsion for GWO and ABC for case-2 for standard deviation of distance in clusters

Case-2 100m^2	**Cluster 1**	**Cluster 2**	**Cluster 3**
GWO	21.61	32.34	10.65
ABC	39.84	60.21	15.56

Fuzzy Logic Membership functions updated by GWO

After applying GWO on three input parameters RE, DNS, DNC , their membership function tuned by GWO for that particular WSN environment are shown in figure 12-13. Updated membership functions of inputs by applying ABC algorithm are shown in figure 14-15.

Figure 12 Updated membership function of input RE by using GWO

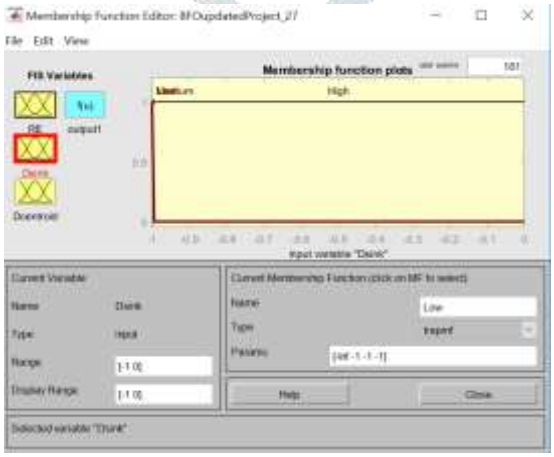

Figure 13 Updated membership function of input DNS by using GWO

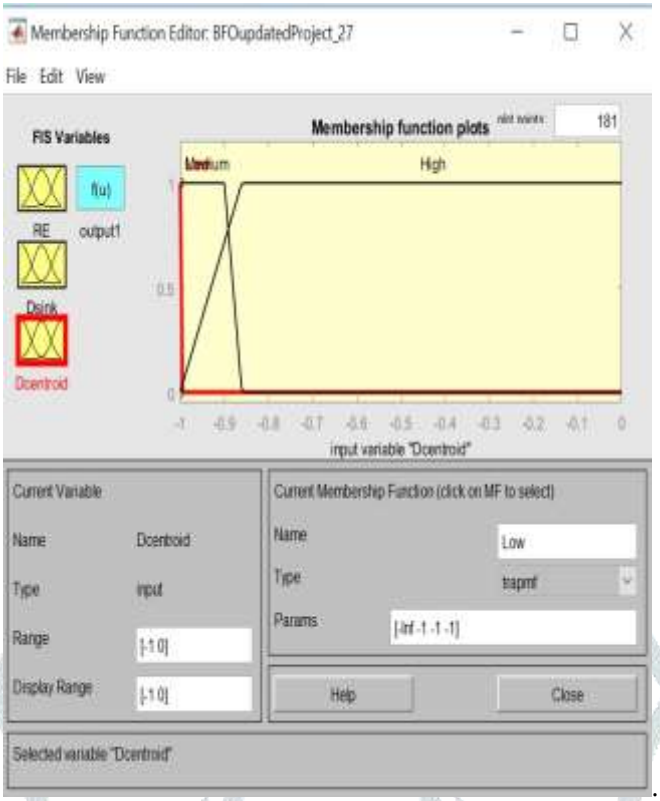

Figure 14 Updated membership function of input DNC by using BFO

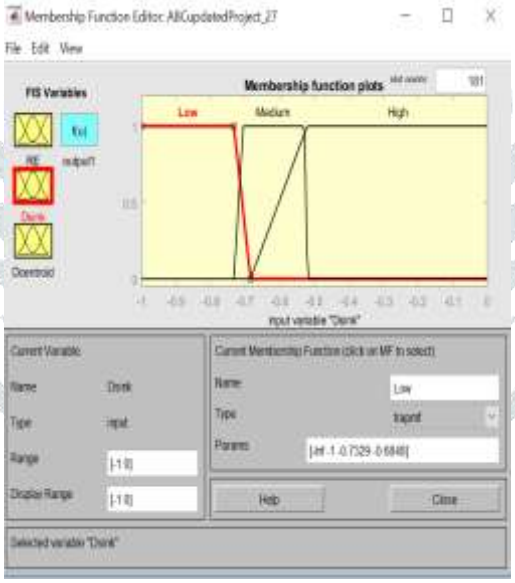

Figure 15 Updated membership function of input DNS by using ABC

Tuned and updated parameters of input functions with GWO and ABC are given here for comparison.

V. CONCLUSION

This work includes the study of clustering, cluster head (CH) selection and other energy efficient communication protocols such as ABC and GWO optimization algorithms for WSN, since it was proposed earlier that clustering improves the residual energy which results in more network lifetime, though we have compared the performance in residual energy. We used Fuzzy logic controller based approach for cluster head choosing and compared performance of GWO and ABC for cluster head selection and improvement of residual energy. It was also found that the GWO tuned Fuzzy controller gives better results than ABC tuned parameters. For clustering, a WSN environment with different geographical area size is considered which is clustered by K-Means technique. We used ABC as a reference to compare the performance of each of the clustering methods. It is concluded that for three different geographical sizes GWO tuned fuzzy logic controller gives improved result in respect of network lifetime in comparison to ABC algorithm. As geographical size increases impact of BFO becomes comparable to that of ABC but for smaller areas GWO should be preferred over ABC for longer network lifetime

REFERENCES

[1] Q. Yu, Z. Luo and P. Min, "Intrusion detection in wireless sensor networks for destructive intruders," *2015 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA)*, Hong Kong, 2015, pp. 68-75.

[2] P. R. Vamsi and K. Kant, "Secure data aggregation and intrusion detection in wireless sensor networks," *2015 International Conference on Signal Processing and Communication (ICSC)*, Noida, 2015, pp. 127-131.

[3] Ajith Abraham, Crina Grosan and Carlos Martin-Vide, "Evolutionary Design of Intrusion Detection Programs," International Journal of Network Security, Vol.4, No.3, PP.328–339, Mar. 2007.

[4] Ioannis Krontiris, Zinaida Benenson, Thanassis Giannetsos, Felix C. Freiling and Tassos Dimitriou, "Cooperative Intrusion Detection in Wireless Sensor Networks.

[5] Djallel Eddine Boubiche and Azeddine Bilami, "CROSS LAYER INTRUSION DETECTION SYSTEM FOR WIRELESS SENSOR NETWORK," International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012.

[6] Shio Kumar Singh, M P Singh and D K Singh, "Intrusion Detection Based Security Solution for Cluster-Based Wireless Sensor Networks," International Journal of Advanced Science and Technology, Vol.30, May, 2011.

[7] A. Anbumozhi, K.Muneeswaran, Sivakasi, "Detection of Intruders in Wireless SensorNetworks Using Anomaly," International Journal of Innovative Research in Science, Engineering and Technology, Volume 3, Special Issue 3, March 2014.

[8] Joseph Rish Simenthy CEng , AMIE, K. Vijayan, "Advanced Intrusion Detection System for Wireless," International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, an ISO 3297: 2007 Certified Organization Vol. 3, Special Issue 3, April 2014.

[9] M. Riecker, A. Barroso, M. Hollick and S. Biedermann, "On Data-Centric Intrusion Detection in Wireless Sensor Networks," *2012 IEEE International Conference on Green Computing and Communications*, Besancon, 2012, pp. 325-334.

[10] F. Bao, I. R. Chen, M. Chang and J. H. Cho, "Trust-Based Intrusion Detection in Wireless Sensor Networks," *2011 IEEE International Conference on Communications (ICC)*, Kyoto, 2011, pp. 1-6.

[11] G. S. Brar, S. Rani, V. Chopra, R. Malhotra, H. Song and S. H. Ahmed, "Energy Efficient Direction-Based PDORP Routing Protocol for WSN," in *IEEE Access*, vol. 4, no. , pp. 3182-3194, 2016.

[12] L. Coppolino, S. DAntonio, A. Garofalo and L. Romano, "Applying Data Mining Techniques to Intrusion Detection in Wireless Sensor Networks," *2013 Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*, Compiegne, 2013, pp. 247-254.

[13] R. Bhargavi, V. Vaidehi, P. T. V. Bhuvaneswari, P. Balamuralidhar and M. G. Chandra, "Complex Event Processing for object tracking and intrusion detection in Wireless Sensor Networks," *2010 11th International Conference on Control Automation Robotics & Vision*, Singapore, 2010, pp. 848-853.

[14] Harmandeep Kaur, "A Novel Approach To Prevent Black Hole Attack In Wireless Sensor Network"International Journal For Advance Research In Engineering And Technology, Vol. 2, Issue VI, June 2014.

[15] Anurag Singh Tomar, "Optimized Positioning Of Multiple Base Station for Black Hole Attack" International Journal of Advanced Research in Computer Engineering & Technology Volume 3 Issue 8, August 2014.

[16] Sowmya K.S, "Detection and Prevention of Blackhole Attack in MANET Using ACO" International Journal of Computer Science and Network Security, VOL.12 No.5, May 2012.

[17] Manvi Arya, "BFO Based Optimized Positioning For Black Hole Attack Mitigation in WSN" International Journal of Engineering Trends and Technology (IJETT) – Volume 14 Number 1 – Aug 2014.

[18] Yash Pal Singh, "A Survey on Detection and Prevention of Black Hole Attack in AODV- based MANETs" journal of information, knowledge and research in computer engineering, nov12 to oct13 ,volume – 02, issue – 02.

[19] Kiran Narang, "Black Hole Attack Detection using Fuzzy Logic" International Journal of Science and Research, Volume 2 Issue 8, August 2013.

[20] Rajani Narayan, "Self-optimization and Self-Protection in AODV Based Wireless Sensor Network" International Journal of Computer Science and Mobile Computing, Vol.3 Issue.1, January- 2014, pg. 244-254.

[21] Binitha S, "A Survey of Bio inspired Optimization Algorithms" International Journal of Soft Computing and Engineering ISSN: 2231-2307, Volume-2, Issue-2, and May 2012.

[22] Jaspreet kaur, "BHDP Using Fuzzy Logic Algorithm for Wireless Sensor Network under Black Hole Attack"International Journal of Advance Research in Computer Science and Management Studies Volume 2, Issue 9, September 2014 pg. 142-151.

[23] SatyajayantMisra, "Blackhole Attacks Mitigation with Multiple Base Stations in Wireless Sensor Networks"IEEEE, 2011.

[24] C.V.Anchugam, " Detection Approach for Black Hole Attack on AODV in MANETs using Fuzzy Logic System" International Journal of Advanced Information Science and Technology Vol.33, No.33, January 2015.

[25] Savita Shiwani, "Detection of Black Hole Attack In MANET Using FBC Technique" International Journal of Emerging Trends & Technology in Computer Science, Volume 2, Issue 2, March – April 2013.

[26] Naveen Kumar, "A Fuzzy Based Approach to Detect Black hole Attack" International Journal of Soft Computing and Engineering ISSN: 2231-2307, Volume-2, Issue-3, July 2012.