JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Comparative Analysis of ABC & GWO Algorithm for Wireless Sensor Network

[1]AMIT GARG, [2] MUKESH KUMAR GUPTA

[1]M.Tech Scholar. [2]Assistant Professor

Department of Mechanical Engineering, CBS Group of Institution, Jhajjar, 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: WSN , ABC ,GWO,ABC

I. INTRODUCTION

The ongoing innovative improvement in the fields of remote correspondence has made conceivable the advancement of ease, low force, and multi-utilitarian sensors that are little in size and correspondence over short separations. A remote sensor arrange is included distinctive sensor hubs, little in size, battery fuelled gadgets that can impart and figure signals with different hubs. These days, a shrewd sensor organize is conveyed in huge numbers to give chance to checking and controlling homes, urban communities and the environmental factors. Moreover, they have a wide scope of uses in giving new innovation to observation, protection field. Sensors consolidated into hardware, structures and the situations are gotten together with the viable transmission of detected information that can offer huge advantages to organization. A sensor arrange is a framework comprise of detecting, registering, and correspondence components that gives a manager the ability to instrument, watch, and respond to occasions and wonders in a predetermined domain. A remote sensor arrange (WSN) contains various passage (or "base station") that can pass data with various sensors hubs by means of a remote association. Data assembled by the hub is compacted and sent to the base station legitimately or whenever required, it utilizes different hubs to move data to the base station. The data which is moved is then used by base station association. In Modern pattern the WSN is the best system as far as research idea. The primary purpose for WSN is the different applications in everywhere throughout the world. The game plan of little size of sensor hubs the physical wonders data can be gather effectively however through other technique it is hard to acquire. The development in smaller scale creation idea decreased the expense of the considerable number of parameters like hubs, expanding organizations of remote sensor systems are normal, with the systems in the end developing to huge quantities of hubs. A Wireless sensor framework can be described as an arrangement of devices that can bestow the information amassed from a checked field through remote associations. The data is sent through various center points, and with an entryway, the data is related with various frameworks like remote Ethernet [1,3].

The security of W.S.Ns could be explored in return viewpoints. These workout portray a hazard system that sees 2 basic kinds of assaulting classes [28 – 30] to be express, (I) thinking about aggressor's area, and (ii) considering attacker's quality. In this examination, the work centered inside ambushes of a WSN. So as to explain those referenced phrasings, the definitions are portrayed underneath: Attacks dependent on aggressor's zone Attacks liable to aggressor's zone: Based on information and favorable circumstances of the assailant, ambushes can be coordinated as insider (inside) and outsider (outer) subordinate upon whether the aggressor is a veritable focal point of the system or not [22]. Ambushes can in like way be named bound and dynamic assaults [19].

1. Inward ambushes: When a genuine center of the framework shows oddly or unlawfully it is considered as an inside attack. It uses the subverted center to ambush the framework which can pulverize or agitate the framework with no issue. A foe by genuinely getting the center point and scrutinizing its memories could get its key devices & produce compose information. Moving toward legitimated keys could empower the assailant to dispatch a couple of kinds of attacks, for instance, counterfeit data imbuement and explicit enumerating, without viably being recognized. All things considered, insider ambushes build up the standard security challenge in remote sensor composes; that is the explanation the sum of these assessment focusing this course, which would be displayed in the going with Chapters.

2. Outer attacks: These ambush is portrayed as the attacked performing by a center point that doesn't have a spot with the framework. Obviously, the aggressor center point doesn't have any inward information about the framework, for instance, cryptographic information.

3. Uninvolved ambushes: The attack doesn't have any quick effect on the framework everything considered outside the framework. Dormant attacks are in spying, or seeing of groups exchanged inside a W.S.Ns whenever the correspondence occurs over a remote channelling. Such sort of attacking doesn't make any break in correspondence phases. The attackers could mix vain bundles to exhaust the beneficiary's batteries, or this could get & genuinely wreck center points. Regularly confirmation and encryption methodology shield such aggressors from expanding any extraordinary access to the framework.

4. Dynamic attacks: such an ambush incorporates aggravation of the standard activities of the framework. It could do info obstruction, alteration, traffic assessment, & traffics checking [13]. Dynamic attacking's are staying, copying, & renouncing of changing and information replay. Ambush reliant on attacker's quality Attacking subject to assailant's quality subject to attacking quality: Attackers might used a no. of sorts of devices to attack the concentrated on compose; these devices have assorted count power, radio recieving wire and various capacities. The 2 fundamental groupings had being perceived by K & Wagner [19] including PC classes & bit classes aggressors.

5. Laptop-class: To dispatch an ambush, aggressors might move toward inconceivable devices, for instance, fastest C.P.U, greater batteries powered, more prominent memories spacing, highest-powered radio transmitter or a delicate gathering mechanical assembly. This gear contraption allows a continuously wide extent of attacking that progressively tough to stopping. These goals might be to running some dead code & hope to take insider realities via sensoring orchestrate or upset compose average limits. For example, Harting et. al. told the best way to remove cryptographically keys from a sensors center point via a JTAG engineer interface rapidly [14].

6. Bit class: Attackers have gotten to in any event one sensor centers with the proportional or equivalent capacities like the sensor center passed on in the framework. They may endeavor to stick a radio association, yet just in the sensor center point's brisk locale. Regardless, these ambushes are continuously obliged since the aggressors endeavor to abuse the framework's vulnerabilities using only the sensor's center point limits.

II. LITERATURE SURVEY

Hafiza Syeda Zainab Kazmi (Vol 18 , 2019) talked about the contributing variables in the presentation of Wireless Sensor Networks (WSNs). Blocked system causes decreased system reaction time, lining deferral and more parcel misfortune. To address this issue, we have proposed a transmission rate control strategy. The present hub in a WSN alters its transmission rate dependent on the traffic stacking data picked up from the downstream hub. Multi arrangement is utilized to control the clog utilizing Support Vector Machine (SVM). So as to get less miss grouping mistake, Differential Evolution (DE) and Gray Wolf Optimization (GWO) calculations are utilized to tune the SVM parameters. The near examination has indicated that the proposed approaches DE–SVM and GWO-SVM are more capable than the other grouping methods regarding order blunder [1].

Satyasen Panda (Vol 5, March 2018) talked about fake honey bee state (ABC) calculation with a grouping model to improve the vitality ability of the system. The ABC calculation can improve the inward elements of the bunch head hubs and sensor hubs in the WSN. The proposed calculation can lessen the vitality dispersal of hubs, balance the vitality utilization across hubs and expand the lifetime of the system. The ABC calculation has less number of control parameters in the target work contrasted with different calculations, so it is easy to actualize in bunched sensor organize. The recreation results demonstrate the prevalence of the ABC calculation thought about over different calculations in expanding the vitality proficiency and life span of the system [2].

Halil Yetgin (Volume 19, Issue: 2 , second quarter 2017) gave another strategy to the interloper can destroy on sensors. It might be perform both hypothetically and for all intents and purposes on a framework variant. The fundamental component of interruption location bother is predictable with the speed of the interloper. The program is right off the bat determine for this we use plate model. A solitary and different detecting recognition components is additionally utilized for the discovery model reason. Some fascinating components with regards to interruption discovery, alongside transmission span, testing length, and the irregular passageway time of the interloper additionally are contemplated [3].

G. S. Brar (vol. 4, 2016) gave the use of T.M.S at hubed degreed & IDS at base-station for the WSN organize. Every hub is carries on as like its neighbor mode which incorporates the group hub just as the record and answering to the base station. The base station breaks down all records for the utilization of IDS. In this a model is structured which can be identified and segregate the malevolent hubs from the other strategy. Reproduction outcomes show the adequacy of this variant [4].

Q. Yu (APSIPA 2015) gave the improvement of an IDP interruption discovery program. For this the three procedures were utilized which are the characterization of hereditary calculation. The plan of IDP should be possible by the GEP , MEP & LGP. Without these three strategies the IDP can't work appropriately in this manner the hereditary calculation assume significant job for building up the programming [5].

S. Rani (vol. 35, Oct. 2015) characterizing the issue in the interruption framework and discover the arrangement of all most exceedingly awful condition. In light of those circumstances we increment a noble calculation for interruption discovery and blessing recreations and tests which show the viability of our technique [6].

A. Jain and B. V. R. Reddy (vol. 82, Issue 1, 2015) another methodology accommodated the interloper location framework. The plan depends on the cross layer cooperation over the system and other significant layers. The vast majority of the challenges expelled by cross layer connection method in the IDS. We have tentatively assessed our device utilizing the NS test system to outline its adequacy in recognizing unique types of attacks at a few layers of the OSI model [7].

C.V. Anchugam (Vol.33, Issue 33, 2015) furnished the productive MAC adapt to following framework which is maintained a strategic distance from in the past procedure. So the new technique created in the gatecrasher location framework for the bunch based WSN [8].

P. R. Vamsi (ICSC 2015) utilized EKF technique for the bogus data in the system. The principle part which is utilized in the technique is sensor. It very well may be control temperature, dampness, voltage. The sensor can investigate the bogus data and afterward EKF writing computer programs is applied. It shows the conduct of close hubs and are anticipating their future states. Utilizing diverse collection highlights (normal, total, max, and min), hypothetical edge cost is determined [9]

H. Yetgin, K. T. K. Cheung (vol. 3, Nov. 2015) gave the half and half interruption location framework (HIDS). The HIDS framework is the mix of cross layer and the EPIDS (Energy Prediction based absolutely Intrusion Detection System) gives the greatest conceivable insurance from the interruption framework. It is utilized for the huge WSN. Likewise by consolidating these two procedures a tremendous WSN also gives the great flexibleness to the WSN framework [10].

Ioannis Krontiris (European Conference on Wireless Sensor Network , pp 263-278, 2015) utilized propelled 3 decentralize light weight that will perform immediately of the sensor hub. This strategy ascertains the assaults from the genuine informational index. At that point these outcomes are contrasted with the other unified plans [11].

A. Anbumozhi (Volume 3, Special Issue 3, March 2014) utilized a propelled model is utilized for the interruption recognition plot and statically techniques additionally utilized for the computation procedure. The outcome is that delicate bogus alert with acknowledge to the base consider limit underneath which a hub is viewed as malignant [12].

I. Butun (vol. 16, no. 1, pp. 266-282, 2014) proposed a directional transmission-based vitality cautious controlling show naming P.D.O.R.P to kept powered confirmation. The given algo show PDORP had the attributes of every quality valuable gathered censoring data m/c & DSR controlling shows. In like way, integration of hereditary check & arterialisation looking through progress is done to given guiding show to get mindful of solidarity green most fitting ways. The overall execution evaluation, appraisal through a hybridization approach of the proposed planning show, gives better last thing including less piece mess up rating, less putoff, significantly least quality use, & highest throughput, that winds up in best QoS & enlarge the lives of the framework [13].

Joseph Rish (Vol. 3, Special Issue 3, April 2014) gave plan to the Wi-Fi systems. The plan is light weighted. The primary specialist is focal operator which perform exact interruption discovery by utilization of record meaning procedure and various Local Agents taking strolls lighter oddity based recognition techniques at the hubs. The standards are applied to the focal specialists and the conduct will be broke down [14].

Harmandeep Kaur (Vol. 2, Issue VI, June 2014) gave the strategy to expulsion of a dark gap assault in MANNET. The calculation is given is for the most part given the discovery procedure to the system. A Wi-Fi framework is utilized for the PC people group that utilizes remote insights associations for interfacing system hubs [15].

Anurag Singh Tomar (Volume 3 Issue 8, August 2014) hereditary calculation streamlining is accommodated the recognition of assaults in WSN organize. It is an exceptionally proficient technique since it can evacuate the dark gap assault. They can control the sensor intrigue and dark empty assault can be limiting by the methodologies. As we're utilizing distinctive BS for transmitting the practically identical information so it calling for added ability to transfer the data so in predetermination we can appearance to chop down the hugeness affirmation of the sensor community focuses [16].

Manvi Arya (Volume 14 Number 1, Aug 2014) proposed a superior than normal strategy that utilizes two or three base stations to be sent each what bearing inside the structure to countering the effect of dull openings on information transmitted. Our beguilement results showing as our methodology would merits farther than 99 pack transported fulfilmenting misuse one or BS & what's more, the accomplishment fault could enlarge for 3 or more noteworthy BSs regardless of the route that there are increment inside the extent of the diminish opening regions. Resultant affirmed that given methodology can be exceptionally powerful in bringing down the impact of area hubs at the overarching conveyance charge of realities parcels and, along these lines diminishing the disappointment percent to an enormous amount [17].

Yash Pal Singh (volume 2, issue 2, Oct 2013) as gave prior the dark empty assault can be identify and evacuate by the calculation in the MANNET framework. In MANNET framework the security is the significant element for the system. With the expansion being used of MANETS, security has end up being an essential necessity to give covered correspondence among cell hubs. MANETs are in danger of differing attacks. It might be utilized as a disavowal of-guarantor assault wherein it can drop the parcels later [18].

III. PROPOSED TECHNIQUE STEP

A bit by bit calculation for the given technique is shown as:

Stage 1. Instate the hub populace irregular positioning & bearings of microbes. Stage 2. Perform K-implies grouping procedure to make bunches of hubs and their centroids.

Stage 3. Make a target work that could compute DNS , RE & DNC , & furthermore pick CH based on RE and computes mean RE of groups and all out hub populace.

Stage 4 Design a FIS System. F.I.S utilizing Sugeno work for 3 information sources DNC , RE & DNS & make their enrollment capacity & setting rule to choose yield.

Stage 5 Initialize irregular places of dark wolves inside the inquiry space limits.

Stage 6 Consider the looking through space measurement as number of participation work esteems to be tuned which is 15 for our situation.

Step 7 For each randomly generated set of membership functions, calculate the objective function as in equation 16.

Step 8. 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.

Step 9 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*

Step 10. The mean of these three best wolves' positions is taken as the updated positions and objective function is calculated again for new membership functions.

Step 11. 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.

Step 12. This process is repeated till all iterations are not exhausted.

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

Following these means in streamlining of GWO, ideal estimations of fluffy controller participation work is accomplished in our work

IV. RESULT ANALYSIS

In Case-3 200mx200m Area

At the point whenever topographical region is 200.00 m2 then we determined & watched effect of GWO &ABC calculation on expanding the WSN liftiming parameter.

In this Result is calculated as

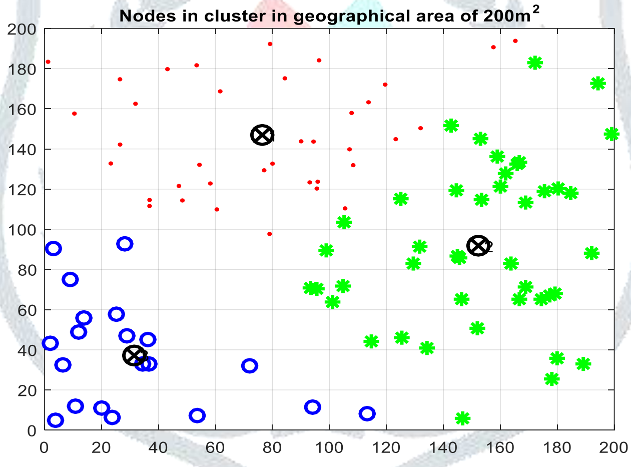

Figure 5.8 200 m^2 Area Clustering of Node

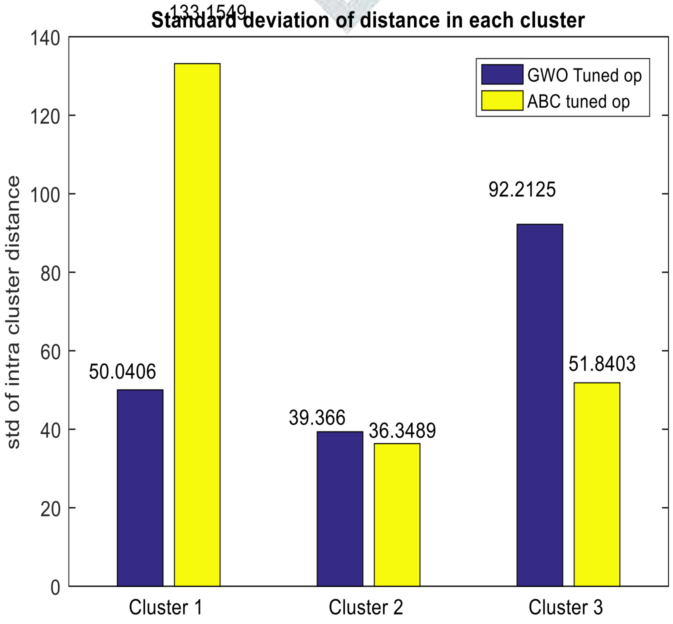

Figure 5.9 S.D Clustering distance

Figure 5.8 In 100 m^2 Area Node Clustering , ABC & GWO Algorithm effect on node for enhancement of lifetime.

Table 5.4 Comparative Analysis for GWO &ABC for case-3 for standard deviation of distance in clusters

Area 200m^2	**C-1**	**C-2**	**C-3**
GWO	50.04	39.36	92.21
ABC	133.15	36.34	51.84

In this C-1, C-2, C-3 are cluster 1 , cluster 2 and cluster 3 respectively.
In case of 200 × 200 m area , GWO algorithm measure S.D for C-1 ,C-2 and C-3 is 50.04 , 39.36 and 92.21 respectively. Similarly , GWO algorithm measure standard deviation for cluster 1 ,cluster 2 and cluster 3 is 133.15 , 36.34 and 51.84 respectively.

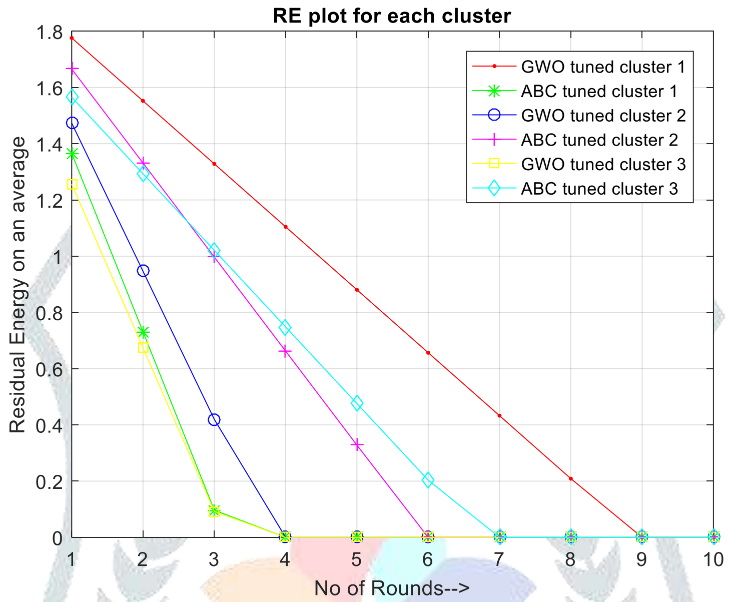

Figure 5.10 RE plot of GWO and ABC

Combined table of all three cases is drawn for better comparison and observation. It tends to be seen that GWO is gives best execution in contrast with proposed algo for continue arrangement of ruling & WSN condition. Moreover perception is this whenever geological territory is enormous at that point aftereffects of BFO and ABC are tantamount, however for little topographical region GWO beat the A.B.C for continue arrangement of ruling, WSN condition.

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. 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.