ISSN No.: 2455-6130
Volume 2, Issue 5, 2017, pp. 10-19

website: www.ijoetr.com

International Journal of Emerging Trends in Research

Energy Consumption Minimization in WSN: A Survey Report

Wafa[1], **Ekta**[2]

[1,2]*Royal institute of management & technology Sonipat, Haryana, 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 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 GSA 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 GSA as an algorithm for clustering of WSN which would result in improved performance with faster convergence.

Keywords: Wireless Sensor Networks; Clustering head selection method; ABC; GSA

1. Introduction

1.1 Wireless Sensor Networks

Sensor nodes offer a powerful mixture of distributed sensing, computing and verbal exchange. The ever-increasing skills of those tiny sensor nodes, which include sensing, statistics processing, and speaking, allow the belief of WSNs primarily based at the collaborative attempt of a number of other sensor nodes. They allow an extensive range of programs and, at the equal time, provide numerous challenges because of their peculiarities, basically the stringent electricity constraints to which sensing nodes are generally subjected. WSNs comprise knowledge and technologies from 3 unique fields; Wireless communications, networking and Systems and Control theory. In order to understand the existing and potential applications for WSNs, state-of-the-art and extraordinarily green communication protocols are required. This chapter offers a first advent to the WSNs, consisting of structure, specific traits and packages.

Surveillance: Suppose multiple networked sensors (e.g., acoustic, seismic, video) are assigned throughout a vicinity consisting of a field of battle. Police investigation package may be designed on prime of this device community to produce records to a quit-user or so the environment.

Within the kind of device community, visitors' patterns are many-to-one, whereby the traffic will vary from raw device statistics to a high stage description of what is happening within the environment, if records process is accomplished domestically.The utility can have some first-rate of supplier (QoS) requirements from the device network, consisting of requiring minimum share device insurance in a vicinity whereby a development is expected to arise, or requiring a most chance of unnoticed detection of an occasion. At the identical time, the community is predicted to produce this nice of carrier for a protracted time (months or even years) the utilization of the strained sources of the community (e.g., device energy and channel bandwidth) whereas requiring little to no out of doors intervention. Meeting these desires requires careful design of both the sensor hardware and the community protocols.

Much more important to detector network operation is electricity-performance, that dictates community period of time, and also the high level QoS, or fidelity, that's met over the direction of the network period of time. This QoS is application-precise and will be measured variety of various strategies. For instance, in a normal police investigation utility, it should be needed that one detector stays active inside every sub location of the network, so as that any entrant is also detected with high chance. During this scenario, QoS may be delineated by means that of the share of the environment that's genuinely blanketed by spirited sensors. in a very normal trailing application, this QoS may be the anticipated accuracy of the goal space estimation provided by means that of the community.

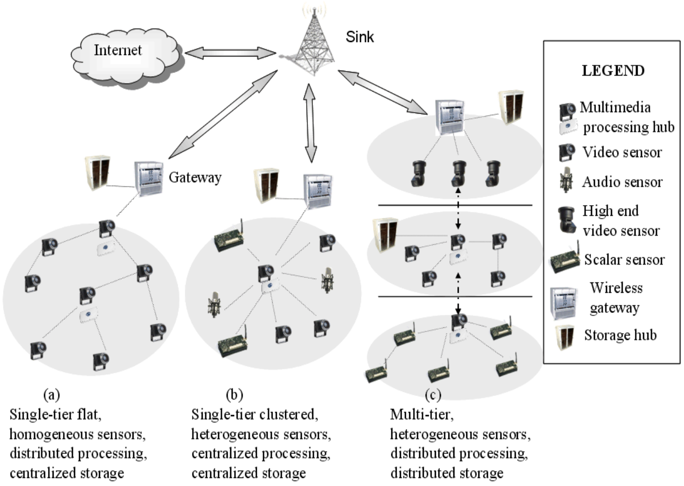

Internet
Sink
Gateway
LEGEND
Multimedia processing hub
Video sensor
Audio sensor
High end video sensor
Scalar sensor
Wireless gateway
Storage hub
(a)
Single-tier flat, homogeneous sensors, distributed processing, centralized storage
(b)
Single-tier clustered, heterogeneous sensors, centralized processing, centralized storage
(c)
Multi-tier, heterogeneous sensors, distributed processing, distributed storage

Figure 1: Wireless Sensor Networking

1.2 Network Protocols

When we style the network protocols for a Wi-Fi detector networks, then numerous sorts of key parts area unit to be thought about. Initial and main, thanks to the scarce power assets, routing choices ought to be guided through a number of awareness of the ability resources within the network. Moreover, detector networks area unit explicit from fashionable advert hoc networks therein contact channels oft exist between activities and sinks, in situ of between man or girl supply nodes and sinks.

The sink node(s) area unit ordinarily larger interested in associate degree traditional description of the environment, as hostile specific readings from the individual detector devices. Thus, communication in detector networks is usually referred to as statistics-centric, rather than cope with-centric, and records could also be aggregate regionally as hostile having all raw records sent to the sink(s). These specific functions of detector networks have implications within the community layer and so need a re-taking under consideration protocols for statistics routing. In addition, sensors typically have understanding in their personal space as how to meaningfully investigate their facts. These neighborhood facts could also be applied among the network layer for routing functions. Finally, if a detector network is correctly connected (i.e., above is required to produce communication paths), topology management services need to be used at the aspect of the everyday routing protocols.

2. Review of Literature

In literature overview, many techniques for improving the energy of the networks were offered; however each of them having their personal boundaries.

Z. Luo *et al.* [1] brought a novel state of affairs in which the intruder can ruin encountered sensors. This scenario is analyzed theoretically and experimentally underneath our system version. The key factor is to talk about the intrusion detection hassle otherwise consistent with the speed of the intruder. We derive the detection chance, which can be carried out to any sensor deployment utilizing the disc model. The detection version used consists of a single-sensing detection model and a multiple-sensing detection model. Some interesting elements in intrusion detection, along with transmission duration, sampling length, and the random entrance time of the intruder also are taken into consideration.

P. R. Vamsi *et al.* [2] offered a comfortable records aggregation framework for Wireless Sensor Networks (WSNs) the usage of TMS at node degree and IDS at Base Station (BS) aspect. Each node inside the network assesses the behaviour of its neighbours using consider rankings and performs the community activities which includes cluster head choice, records aggregation, and reporting to the BS. Then, BS analyzes the acquired records the use of IDS and reports the facts about the malicious sports again to nodes within the network. In this manner, the proposed model identifies and isolates the malicious nodes from the records aggregation technique. Simulation consequences show the effectiveness of this version.

Ajith Abraham *et al.* [3] proposed the improvement of an Intrusion Detection Program (IDP) that can discover recognized assault patterns. An IDP does no longer do away with using any preventive mechanism however it works because the remaining shielding mechanism in securing the device. Three editions of genetic programming techniques specifically Linear Genetic Programming (LGP), Multi-Expression Programming (MEP) and Gene Expression Programming (GEP) had been evaluated to design IDP. Empirical effects display that genetic programming technique should play a major function in developing IDP, which are mild weight and accurate whilst in comparison to some of the traditional intrusion detection systems based totally on system studying paradigms.

Ioannis Krontiris *et al.* [4] defined the trouble of intrusion detection and discover vital and enough conditions for its solvability. Based on those situations we increase a time-honored algorithm for intrusion detection and gift simulations and experiments which show the effectiveness of our method.

Djallel Eddine Boubiche *et al.* [5] proposed a new intrusion detection machine based on cross layer interaction among the network, Mac and physical layers. Indeed we've addressed the trouble of intrusion detection in a different way wherein the idea of cross layer is widely used main to the birth of a new form of IDS. We have experimentally evaluated our gadget using the NS simulator to illustrate its effectiveness in detecting one-of-a-kind forms of assaults at a couple of layers of the OSI model.

Shio Kumar Singh *et al.* [6] proposed a new method of an Intrusion Detection Based Security Solution for Cluster-Based Wireless Sensor Networks. In the proposed method, an efficient MAC cope with based totally intruder tracking gadget has been evolved for early intruder detection and its prevention.

A. Anbumozhi *et al.* [7] proposed an Extended Kalman Filter (EKF) mechanism to filter out the false statistics in sensor network. The fake data may be acted by some occasion specifically malicious, emergency event. Malicious event are acted by means of intruders, and Emergency event are acted by using a few coincidence incidence e.G. Fire. In this paper, Sensors are used to experience the temperature, humidity, mild, voltage and so forth in a selected vicinity. Intruders make the sensors to get the false analyzing therefore EKF mechanism is proposed. EKF video display units the behaviour of neighbours and are expecting their future states, every node ambitions at putting in ordinary variety of the neighbour’s future transmitted aggregated values. Using different aggregation features (average, sum, max, and min), theoretical threshold price is calculated.

Joseph Rish Simenthy *et al.* [8**]** proposed a Advanced Intrusion detection device wherein the Hybrid Intrusion Detection System(HIDS), Energy Prediction based totally Intrusion Detection System (EPIDS) as well as the Cross layer Detection System are carried out In various degrees on the way to assure maximum possible protection from the Intrusions. Energy Prediction Approach by myself is not appropriate for the WSN, so HIDS which is appropriate for large and sustainable WSN’s is combined. Also combining these two techniques together with the Cross Layer IDS make it appropriate for a huge WSN additionally. So the new proposed IDS will provide a huge range of flexibleness for its utility in any form of Wireless Sensor Networks.

M. Riecker *et al.* [9] advanced 3 decentralized, light-weight information anomaly detection mechanisms that can be run without delay on sensor nodes. These algorithms are evaluated with a real dataset to which we brought plausible attacks. Further, they're as compared to conventional centralized anomaly detection mechanisms.

J. H. Cho *et al.* [10] proposed a believe based totally intrusion detection scheme using a quite scalable hierarchical consider management protocol for clustered wireless sensor networks. In this paper, advanced an analytical model based on stochastic Petri nets for performance evaluation of the proposed trust-based totally intrusion detection scheme, as well as a statistical method for calculating the false alarm possibility. We examine the sensitivity of false alarms with appreciate to the minimum consider threshold beneath which a node is considered malicious. Our consequences display that there exists an best consider threshold for minimizing fake positives and fake negatives.

G. S. Brar *et al.* [11] proposed a directional transmission-based energy aware routing protocol named PDORP to keep power intake. The proposed protocol PDORP has the traits of each strength efficient gathering sensor information machine and DSR routing protocols. In addition, hybridization of genetic algorithm and bacterial foraging optimization is carried out to proposed routing protocol to become aware of strength green most appropriate paths. The overall performance evaluation, assessment thru a hybridization approach of the proposed routing protocol, gives better end result comprising less bit error rate, less put off, much less strength consumption, and higher throughput, which ends up in better QoS and extend the life of the community.

L. Coppolino *et al.* [12] proposed a hybrid, light-weight, dispensed Intrusion Detection System (IDS) for Wi-Fi sensor networks. This IDS uses each misuse-primarily based and anomaly-based totally detection techniques. It consists of a Central Agent, which plays especially accurate intrusion detection by the use of records mining techniques, and a number of Local Agents going for walks lighter anomaly-based detection strategies at the motes. Decision bushes have been adopted as type set of rules within the detection procedure of the Central Agent and their behaviour has been analysed in selected attacks situations.

R. Bhargavi *et al.* [13] proposed a CEP (Complex Event Processing) primarily based software for object detection tracking in Wireless Sensor Network (WSN) surroundings. Also the detection of an interloper the use of semantic question processing is proposed. CEP is a rising technology within the discipline of data processing and identifying patterns of interest from a couple of streams of activities. CEP is utilized in development of packages which must deal with voluminous streams of incoming information with the mission of finding significant activities or styles of activities, and respond to the occasions of hobby in real time. ESPER, an open source Complex Event Processing engine is used to expand the software.

Harmandeep Kaur *et al.* [14] proposed a unique technique to discover and prevent black hole attack in MANET. In the Wi-Fi networks, radio conversation is the medium of desire. A Wi-Fi community is any form of pc community that uses wireless statistics connections for connecting network nodes. It lets in humans to get admission to and talk to exceptional gadgets without any wants of wires. In the MANET, exceptional forms of attacks are viable. These attacks are classified as: energetic assaults and passive attacks.

Anurag Singh Tomar *et al.[*15] proposed the algorithm so as to help to efficiently deliver the packets in the presence of black hollow assault by means of way of using a couple of base stations with optimized feature using genetic set of policies (GA). They also allow the manipulation of sensor interest, so safety is essential issue as kind of attacks are gift within the network for taking pictures the information. One of the attacks is black hollow. As we're using multiple Base Station (BS) for sending the equal data so it calls for added electricity to send the information so in destiny we are able to appearance to lower the energy intake of the sensor nodes.

Sowmya K.S *et al.* [16] proposed a method to discover and prevent black hollow attacks via the use of notifying exceptional nodes within the community of the incident. With the increase in use of MANETS, safety has turn out to be a vital requirement to provide blanketed communication among cell nodes. To conquer the challenges, there's a want to construct a multifence safety answer that achieves each great protection and proper network standard performance. MANETs are at risk of diverse assaults. It may be used as a denial-of-issuer attack wherein it can drop the packets later.

Manvi Arya *et al.* [17] proposed a good technique that uses a couple of base stations to be deployed every which manner within the network to counter the impact of black holes on data transmission. Our simulation consequences show that our method will advantage further than 99 packet transport fulfilments victimization one or base stations and moreover, the achievement charge can increase with three or larger base stations even though there is increase within the radius of the black hole region. Results confirmed that our approach could be very effective in lowering the effect of location nodes at the prevailing delivery charge of facts packets and, therefore decreasing the failure percent to a large quantity.

Yash Pal Singh *et al.* [18] supplied a survey of projected techniques of detective work region assault closer to ad -hoc on-name for distance vector routing protocol in cell ad hoc networks. In a very black hollow assault, a malicious node answers every path request with a pretend reply claiming to own the shortest and most up to date direction to the vacation spot. However, while the records packets arrive, the malicious node discards them. Several detection techniques rectangular measure outlined and their strengths and weaknesses referred to. Manet rectangular measure very in chance of Attack resulting from their dynamically ever-changing topology, absence of historical safety infrastructure and open medium of spoken communication, that in contrast to their stressed opposite numbers cannot be at ease, stingy or malicious nodes may additionally do supposed packet dropping misbehaving.

Kiran Narang *et al.[*19] Furnished the answer in the direction of black hollow attack this is primarily based on fuzzy rule .Fuzzy rule based totally answer discover the inflamed node similarly to offer the answer to lessen records loss over community. MANET is a dynamic community with massive type of mobile nodes .As the web page traffic will increase over the manet it will outcomes in massive sort of problems. One in each of attack is black hole assault .As a end result a few packet loss over the community and slows the communiqué method. The fuzzy commonplace enjoy is carried out on packet loss and facts fee at time of node communication. Now on this it will ship the packet from surrounding nodes. This algorithm will offer the better answer.

Rajani Narayan *et al.[*20] provided techniques of integration of autonomic computing requirements into WSNs. PSO based definitely clustering for self-optimization and watch mechanism primarily based technique for self-protection from black hole attack has been offered. He proposes a completely unique approach for transactional protection with chaos primarily based AES cryptography. The proposed approach for self-optimization makes use of PSO based cluster head choice for green community lifetime. Results show that proposed device outperforms the winning cluster head choice techniques in terms of network throughput, stop to end transport ratio and network lifetime.

Binitha S *et al.* [21] offered a huge assessment of biologically stimulated optimization algorithms, grouped with the assist of the natural concern that's inspired individual and all regions in which the ones algorithms had been most effectively carried out. In words, almost both of the EA and SI algorithms carry out in a complex manner. It can be very drastic and has been performed to immoderate optimization troubles in laptop networks, control structures, bioinformatics, information mining, exercise concept, tune, biometrics, power systems, picture processing.

Jaspreet kaur *et al.* [22] proposed BHDP (Black Hole Detection and prevention the use of fuzzy excellent judgment algorithm) that used detects and stops the black hollow assault in WSN. The benefit of the proposed set of regulations is that it does no longer make any amendment to the packet. Hence the a couple of base stations get keep of the identical packet regardless of the presence of black hollow. The parameters (along with packet delivery ratio, overall packet drop, routing over head, theoretical packet) used on this artwork to assist in decide the outcome of black hole assault efficiently at the Wi-Fi sensor community.

Satyajayant Misra *et al.* [23] proposed companion cost-effective approach that makes use of a couple of base stations deployed within the community to counter the impact of black holes on information transmission. Our simulation effects display that our approach will get over 99 packet shipping accomplishment. His subject matter will find out a hundred of the black hole nodes and exhibit with the assist of simulation results that the tactic suffers from very little faux positives. BAMBi is based at the guidance of over one base stations at durations the community and routing of copies of records packets to those base stations. It is truly powerful and desires little or no computation and message exchanges at periods the network, therefore saving the strength of the SNs.

C.V. Anchugam *et al.* [24] proposed to stumble on the assault by way of using detection machine that makes use of FIS for routing protocol. FIS offers a natural way of representing and reasoning the troubles with uncertainty and imprecision. As the assessment cease end result suggests that the proposed gadget is acting better than cutting-edge routing set of rules in case of packet supply ratio, via positioned, surrender-to-quit put off so we are able to say that fuzzy commonplace feel does solves the hassle of malicious node inside the community and eventually increases the overall normal performance of the community.

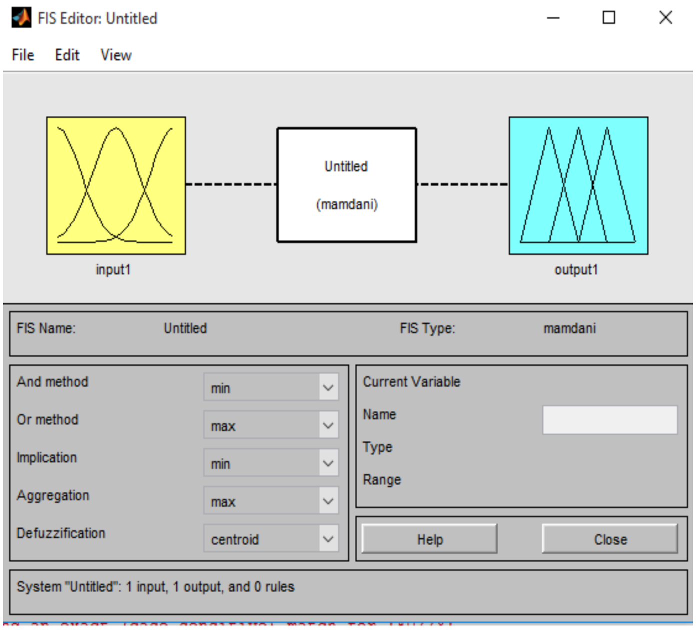
Savita Shiwani *et al.* [25] Studied the black hole attack, beneath the AODV routing protocol and its effect are careful by asserting but this attack disrupt the general overall performance of Edouard Manet and what is greater studied of the effect of area attacks in Edouard Manet the utilization of every reactive and proactive protocols and to in shape the vulnerability of every the ones protocols in competition to assault. The soliciting for node analyses the behaviour of unknown node the usage of fuzzy approach and on the concept of ending the node takes this node inside the direction of the packet. After, states of the nodes in addition are frequently used by the routing protocol to skip the ones malicious nodes. Our method suggests that in an incredibly dynamically converting community, this approach will come upon most of the malicious nodes with a reasonably excessive extremely good charge. The packet transport rate a few of the Edouard Manet additionally could also be extended thus.

Naveen Kumar *et al.* [26] furnished a fuzzy primarily based definitely choice to test a node is infected via Black hollow attack or node. The proposed gadget will pick out the attack over the node further to offer the answer to reduce the records loss over the community. A Wireless community is a dynamic community with massive no. of nodes. As the traffic increases over the network such form of network suffers from the troubles like congestion and packet loss. The packet loss is appropriate up to three threshold rate but as there can be more packet loss we need a few solutions for this. The equal solution is supplied in this paper. Here we're imparting a fuzzy based choice to test a node is inflamed thru the use of Black hollow assault or node.

3. Overview of Fuzzy Logic Technique

The concept of Fuzzy Logic (FL) became conceived by using LotfiZadeh, a professor at the University of California at Berkley, and offered now not as a control methodology, however as a manner of processing facts through allowing partial set club in place of crisp set club or non-membership. Fuzzy logic is an extension of Boolean logic based totally on the mathematical idea of fuzzy sets, that's a generalization of the classical set idea. By introducing the belief of diploma inside the verification of a situation, accordingly permitting a condition to be in a state aside from actual or fake, fuzzy common sense provides a totally precious flexibility for reasoning, which makes it viable to keep in mind inaccuracies and uncertainties. One advantage of fuzzy logic a good way to formalize human reasoning is that the guidelines are set in natural language. This technique to set theory changed into no longer applied to manipulate structures until the 70's due to insufficient small-pc functionality previous to that time. Professor Zadeh reasoned that people do now not require precise, numerical records input, and but they may be capable of enormously adaptive manage.

In this context, FL is a hassle-solving manage device method that lends itself to implementation in systems starting from easy, small, embedded micro-controllers to huge, networked, multi-channel PC or computer-primarily based records acquisition and control structures. It can be applied in hardware, software program, or a combination of each. FL affords an easy way to reach at a specific end based upon vague, ambiguous, obscure, noisy, or missing input information. FL's method to control issues mimics how someone would make selections, simplest an awful lot quicker. As the complexity of a machine will increase, it becomes more difficult and in the end impossible to make a particular statement about its behavior, subsequently arriving at a factor of complexity in which the bushy common sense approach born in humans is the best manner to get on the trouble.



FIS Name: Untitled

FIS Type: mamdani

And method: min

Or method: max

Implication: min

Aggregation: max

Defuzzification: centroid

System "Untitled": 1 input, 1 output, and 0 rules

Figure 2: Fuzzy logic graphical interface of MATLAB's toolbox

The default system has one input and one output and makes use of the Mamdani inference and aggregation approach. This editor additionally illustrates the three elements of a fuzzy controller; fuzzification, inference, and defuzzification. To begin, let us outline the membership functions. Double click on the yellow enter box and you'll be delivered to the membership feature editor.

4. Conclusion

Our thesis work includes the study of clustering, cluster head (CH) selection and other energy efficient communication protocols such as ABC and GSA optimization algorithms for WSN, since it was proposed earlier that clustering improves the network lifetime. We used Fuzzy logic controller based approach for cluster head choosing and compared performance of GSA and ABC for cluster head selection and improvement of network lifetime. It was also found that the GSA 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 GSA tuned fuzzy logic controller gives improved result in respect of network lifetime in comparison to ABC algorithm. As geographical size increases impact of GSA becomes comparable to that of ABC but for smaller areas GSA 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 Sensor Networks 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, 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