Anuradha, 2022, 10:4
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

Performance Enhancement of Wireless Sensor Network Using GWO Algorithm

M.Tech. Scholar Km Anuradha, Asst. Prof. Asst. Prof. Hemlata
Department of Computer Science,
IITM Group of Institution,
Murthal, Sonipat

.

Abstract- The enormous potential for sensor networks to link the real world with the virtual world has skyrocketed the interest in Wireless Sensor Networks (WSN). Due to the fact that many sensor devices use battery and node energy, changing them might be a challenge. As a result, increasing the energy efficiency of these networks, or their "lifespan," becomes critical. A fuzzy logic controller is used to increase WSN energy efficiency through clustering and the selection of cluster heads. On the basis of network longevity, it does a comparison of the various ways. It compares the Gray wolf optimization (GWO) algorithm with the current ABC optimization approach for various network sizes and scenarios. It offers a high-performing and computationally simple approach for selecting cluster heads. In addition, it offers GWO as a clustering technique for WSN, which would increase performance and convergence more quickly.

Keywords- WSN, ABC, GWO.

INTRODUCTION

Remoting sensors that are small in size and can communicate across short distances have been developed as a result of the continual evolution of remote communication technology. An arrangement of distant sensor hubs, all of which are battery-powered and small in size, may communicate and figure signals with each other.

These days, a clever sensor network is delivered in large numbers to enable homeowners, urban areas, and environmental elements the chance to be checked and controlled. In addition, they have a wide range of applications in the realm of surveillance and protection.

Sensors that are integrated into hardware, buildings, and environments are able to transmit information that can have a significant impact on an organization's bottom line. Using a sensor set, a manager may monitor, record, and respond to events and discoveries inside a predefined domain by means of a framework composed of detection, registration, and correspondence components.

Using a distant association, a sensor network (WSN) may transmit data to and from numerous hubs via a variety of passages (or "base stations"). In order to transport data to the base station, several hubs are used to compile and send the data gathered by the hub. The base station association uses the data that is sent.

The WSN is the greatest system for research in the Modern pattern. WSN's major goal is to support a wide range of global applications. Physical wonders data can be gathered effectively by the use of small sensor hubs, but it is difficult to get using other methods. Many factors, such as hubs, have been reduced in cost via the growth of smaller-scale creative ideas.

As remote sensing system organizations increase, the systems themselves eventually grow to large amounts of hubs. In the context of a wireless sensor framework, this is a collection of devices that may transmit data gathered from a monitored area via distant connections. The data is routed through multiple hubs and connected to various frameworks, such as distant Ethernet, via an entrance [1, 3].

International Journal of Science, Engineering and Technology

An Open Access Journal

W.S.N. security might be examined from a variety of perspectives. There are two main types of attacking classes [28–30]: (I) think about the aggressor's location, and (ii) thinking about the aggressor's quality. The focus of this investigation was on WSN ambushes. For the sake of clarity, the following definitions are provided for each of the cited expressions: attacks based on the aggressor's zone of operation Aggressor-zone attacks include the following: Ambushes can be organized as insider (inside) and outsider (outside) subordinates depending on whether the attacker is a veritable focal point of the system [22]. An ambush can also be referred to as a "bound and moving attack."

In-house snares: It's called an inside assault if a critical component of the system appears out of the ordinary or illegally. It may pulverize or agitate the framework with ease since it ambushes it with the corrupted center. This information can be obtained by an adversary who has gained access to the system's core by infiltrating its memory and performing memory-scanning operations. Shifting to legitimated keys could provide an attacker more leeway in their attacks, such as data forgery and explicit enumeration, without being detected.

Considering the fact that insider ambushes are a common security issue in remote sensor compositions, this course's assessments, which will be shown in the following chapters, will focus on this.

When an assault comes from the outside, it's depicted as a center point that doesn't belong anywhere in the structure. For obvious reasons, the aggressor center point has no access to the framework's internal information, such as cryptographic information.

Ambushes that have no immediate impact on the framework are known as uninvolved ambushes. When communication takes place over a distant channel, dormant assaults take the form of spying or viewing groups exchanged inside a W.S.Ns. Such a tactic doesn't interrupt the flow of communication in any way. Assailants might use a combination of ineffective bundles to drain the beneficiary's batteries or they could use this to gain and seriously damage the center points. There are several security measures in place to prevent these types of threats from gaining any unusual access to the framework.

Dynamic attacks: this type of ambush includes amplification of the framework's normal actions. It has the ability to hinder, change, appraise, and check traffic [13]. Staying, copying, and renouncing change and information replay are the hallmarks of dynamic attacks. A successful ambush is heavily dependent on the attacker's abilities. The quality of the assailant's attack is dependent on the quality of the attack itself: Many different types of assault devices, each with a different number of count power, radio receiving wire, and capacity, might be employed to attack the targeted composition. According to K and Wagner [19], PC classes and bit classes of aggressors were two major groups.

When planning an ambush, aggressors may use equipment that are out of this world, such as the quickest central processing unit (CPU), the largest battery capacity, the most conspicuous memory space, the most powerful radio transmitter, or a delicate mechanical assembly. This contraption's gears allow for an increasingly broad range of attacks that is more difficult to halt.

There are a number of possibilities for these aims, including running some dead code and attempting to take insider realities by sensoring or disrupting the composition of average limitations using sensors. When it comes to removing cryptographic keys from a sensor center point through a JTAG engineer interface, for example, Harting et al. explained the optimum method.

At least one sensor center with the same or similar capabilities as the sensor center in the framework has been accessed by attackers. They may try to establish a radio link, but only in the vicinity of the sensor center point. As a result of the attackers' constant attempts to exploit the framework's weaknesses by utilizing the sensor's center point constraints, these ambushes are unavoidable.

II. LITERATURE SURVEY

Wi-Fi Sensor Networks: Contributing Factors in the Presentation by Hafiza Syeda Zainab Kazmi (Vol. 18, 2019) (WSNs). System response time is reduced, line delays occur, and package mishaps increase as a result of a blocked system. We've come up with a transmission rate management approach to deal with this problem. Depending on the traffic stacking data received from the downstream hub, the current

International Journal of Science, Engineering and Technology

An Open Access Journal

hub in a WSN might change its transmission rate. Support Vector Machine (SVM) is used to clear a blockage using a multi-arrangement approach (SVM). With the help of DE and GWO calculations, it is possible to fine-tune the SVM parameters and reduce miss grouping errors. There is evidence that the suggested approaches DE–SVM and GWO- SWM are more equipped to handle order blunder [1] than the other grouping methods.

Using a grouping model, Satyasen Panda (Vol 5, March 2018) discussed how to boost the system's vitality by calculating the fake honey bee state (ABC). As a result of ABC calculations, the inner parts of the WSN sensor and bunch heads can improve. With the suggested computation, it is possible to reduce hub vitality distribution, equalize hub vitality usage, and lengthen the system's lifespan. Compared to other calculations, the ABC calculation contains fewer control parameters in the target job, making it easier to implement in a sensor cluster. The simulation results show that the ABC calculation is preferred over other calculations in terms of increasing the system's energy efficiency and lifespan [2].

When an intruder is able to disable sensors, Halil Yetgin (Volume 19, Issue: 2, second quarter of 2017) offers another technique for destroying the interloper. Hypothetically, it may be done on a different framework variation as well as practically. The interloper's speed is a reliable predictor of where the interruption will occur. We employ a plate model in the software from the start. The discovery model makes use of both a single and a variety of detecting and recognizing components. An interloper's irregular passageway duration is also taken into consideration [3], along with transmission span, testing length and other intriguing components related to interruption discovery.

To structure the WSN, G. S. Brar (vol. 4, 2016) recommended using T.M.S. at hubed degrees and IDS at base stations. Every hub operates in the same manner as its neighbor, incorporating the group hub as a record and responding to the base station, which is the case for every hub. The base station breaks all previous records for IDS usage.

As a result of this, a model has been created that may be used to identify and isolate the hubs of evil. This variant's effectiveness in reproduction has been demonstrated [4].

There were improvements made to IDP interruption detection software by Q. Yu (APSIPA 2015). The three processes that characterize hereditary calculation were employed in this case. The GEP, MEP, and LGP should be able to support IDP's strategy. In order for the IDP to function well, the hereditary calculation must take on a prominent role in the development of the programming [5].

As described by S. Rani (vol. 35, oct. 2015), the problem with the interruption structure and how to fix the most horrendous conditions are both addressed here. For this reason, we have increased our wonderful calculation for interruption discovery and blessing recreations that demonstrate the feasibility of our method [6].

According to Jain and Reddy (vol. 82, 2015, issue 1), a different approach might be used to account for the intruder location. There is a need for cross-layer coordination in order for the strategy to succeed. The IDS's cross-layer connection mechanism eliminates the great majority of problems. We have tested our device using the NS test system to see if it is capable of identifying specific sorts of assaults at a few OSI model levels [7].

Anchugam (Vol.33, Issue 33, 2015) provided the successful MAC adaptability to the following structure, which was previously avoided. That's why we've developed a brand-new method in our location architecture for WSNs using the gatecrasher [8].

He used EKF to remove fraudulent data from the system, as reported by P. R. Vamsi (ICSC 2015). The sensor is the most important component of the method. This might very well be a way to regulate things like temperature, humidity, and even voltage. For this reason, EKF authoring computer programs is used in conjunction with sensors that can detect false data. It depicts the behavior of nearby nodes and predicts what they will become in the future. The potential edge cost is calculated by using a variety of collection highlights (normal, total, maximum, and minimum) [9].

Half and half interruption location framework was given by H. Yetgin, K T K Cheung (vol. 3, Nov. 2015). (HIDS). Cross-layer and EPIDS (Energy Prediction-based Absolute Intrusion Detection System) combine to form the HIDS framework, which provides the

highest level of interruption-based insurance possible. The WSN uses it. Similarly, the WSN structure gains a great deal of adaptability by combining these two techniques into one massive WSN [10].

Decentralized, light-weight propelled 3 sensor hubs were used by Ioannis Krontiris (European Conference on Wireless Sensor Network pages 263-278, 2015). Using this method, the actual informational index is used to determine which attacks have been launched. Those outcomes are compared to the other unified plans at that moment.

For the interruption recognition plot, A. Anbumozhi (Volume 3, Special Issue 3, and March 2014) used a propelled model, as well as statically approaches, for the computing procedure. As a result, a malignant hub is labeled as a sensitive false alarm with acknowledgement of the fundamental consider limit [12].

P.D.O.R.P., a directional transmission-based vitality careful controlling show, was proposed by I. Butun (vol. 16, no. 1, pp. 266-282, 2014) to keep powered confirmation. PDORP possessed all the qualities of a worthwhile censoring data m/c and DSR-controlling display, as demonstrated by the algo. Also, to help people become more aware of the importance of solidarity green, the integration of genetic testing and arterializations scanning is being carried out. According to provided planning demonstrate, an overall execution evaluation that includes fewer piece mess-up rating and less put-off, as well as the lowest quality usage and the maximum throughput results in optimal QoS and longer framework lifespan [13].

Joseph Rish (Vol. 3, Special Issue 3, April 2014) devised a strategy for Wi-Fi networks. It's a light-weight strategy. Focal operator performs precise interruption finding using record-meaning method and various Local Agents at the hubs using oddity-based identification approaches. The focus experts will be held to the same standards and their behavior will be scrutinized [14].

Expulsion of a dark gap assault in MANNET was described in detail by Harmandeep Kaur in Vol. 2, Issue VI, June 2014. The discovery process is largely used in the computation provided. A Wi-Fi framework is used by PC users who rely on distant information connections to connect system hubs [15].

As a result of Anurag Singh's efforts (Volume 3 Issue 8, August 2014) In the WSN framework, hereditary calculation streamlining is used to recognize attacks. It is a highly effective tactic since it eliminates the dark gap attack. Sensor intrigue and dark emptiness assault can be controlled, but the methods used to do so can be restrictive for them. Preliminary analysis shows that we can reduce sensor community focus size by using different BS for delivering the nearly equivalent information [16] since the more data transmission capacity is required.

Using two or three base stations, Manvi Arya (Volume 14 Number 1, Aug 2014) came up with a better-than-average technique to mitigate the effect of boring openings on information broadcast. This study's beguilement results show that our methodology merits more than 99 packs of transported fulfillment misusing one or more BSs, and furthermore, the achievement fault could grow for three or more notable BSs regardless of how much growth there is inside the extent of shrinking opening regions Overall conveyance charges for real estate parcels can be reduced by as much as 70 percent when using this technique, according to Resultant [17], which states that the methodology is extraordinarily effective in doing so [18].

Yash Pal Singh is (volume 2, issue 2, Oct 2013) the computation in the MANNET framework may be used to detect and evacuate the dark empty attack, as was previously mentioned. The most critical component of the MANNET framework is its security. Secure communication between cell hubs has become a need as the use of MANETS has increased. Different types of assaults can be launched against MANETs. An attack against the guaranteeor might be used to dump shipments 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

International Journal of Science, Engineering and Technology

An Open Access Journal

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

1. 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

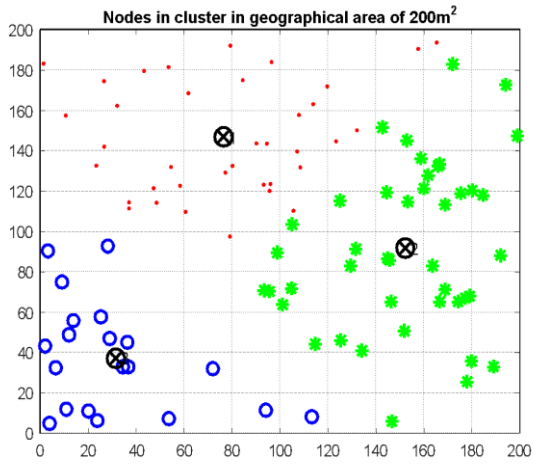

Fig 1. 200 m2 Area Clustering of Node.

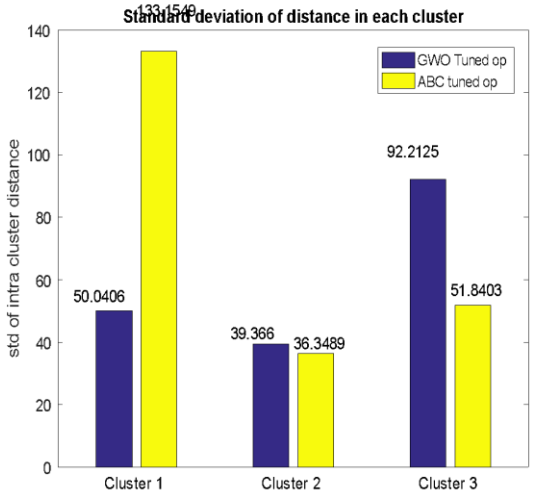

Fig 2. S.D Clustering distance.

Figure 5.8 In 100 m2 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 200m2	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

International Journal of Science, Engineering and Technology

An Open Access Journal

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.

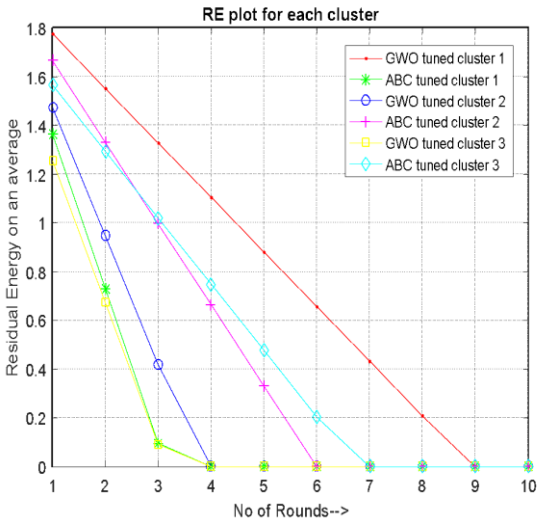

Fig 3. RE plot of GWO and ABC.

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 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, 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] Satyajayant Misra, "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.