Ritu Mehta *et al*, International Journal of Computer Science and Mobile Applications,
Vol.3 Issue. 6, June- 2015, pg. 01-11 **ISSN: 2321-8363**

IDS in WSN Based on Spy Node and Voting Scheme

Ritu Mehta, Mr. Vinod Saroha(Guide)
mehta.ritu27@gmail.com
Computer Science and Engineering (Network Security)
B.P.S M.V., Khanpur Kalan Haryana, India

Abstract- Now a day's wireless Sensor network is latest technology for data transmission but due to the open design environment of the WSN it is vulnerable to various types of attack and because it is used in various critical application like health care, smart building, industrial application, smart grids and energy control system etc. Thus there is a necessity of a mechanism that prevents these attacks i.e. intrusion detection system. In this paper we mainly focus in ids in WSN environment that is based on spy node and voting based mechanism show implementation result which describes the effectiveness of our ids as compare to normal ids in WSN environment.

Keywords-WSN, IDS, Spy node, voting based IDS

1. INRODUCTION

Wireless Sensor Network is a latest technology which, Health or medical application, Industrial monitoring, Structural strength monitoring etc. Over the years, it has been emerged as a competent technology. WSN has a group of sensor nodes which are deployed over the area of application and provided with energy sources for its efficient working. Sensor nodes differ in their characteristics like separation distance, energy level etc based on the application area. In other words we can say that they are application dependent. Also WSNs are vulnerable to many types of security attacks. This is because of transmission medium's broadcast nature. Also WSNs

have additional vulnerability because nodes are placed in areas prone to physical attacks or open environment.

Many security solutions for WSNs have been proposed by many researcher, they are authentication, key exchange, and secure routing. These are only capable of ensuring security up to certain level. These cannot detect or eliminate all the security attacks. So an Intrusion Detection System (IDS) is considered as the foremost solution to address wide range of security problems. Almost all IDSs can only detect the attacks or intrusions. They cannot prevent them or eliminate them. So as discussed earlier an IDS will detect such activities. The main function of the IDS is to keep an eye on the user's activities and network behavior at different layers. No IDS is capable of giving a perfect solution for the intrusions. So a combination of 2 or more IDSs is found to be efficient. So in order to achieve a perfect defense from the intrusions, different IDSs should be employed at different levels in order to meet the accuracy.

2. PROBLEM FORMULATION AND OBJECTIVES

Problem description: WSN suffers from various attacks by anomaly nodes. These nodes are stated as intruders which can alter the message passed to base station. As WSN is used in various applications like in emergency data transfer, military applications, surveillance etc. so requirement of accurate information is necessary, but if any intruder is active in the network and unidentified then false information can be transferred to head which may lead to dire consequences. So it is necessary to detect these anomaly nodes. For this many problems are faced some of them which are considered in our work, after research survey are listed below.

- WSN is a resource constrained and energy constrained network. So there is always scarcity of resources and battery in sensor nodes so conventional IDS can't be used for WSN.
- Many IDS presented by researchers are limited to only network layer due to which many types of attacks by intruders may go unidentified. So detection scheme should be such

that it can analyze the anomaly node at each OSI layer so that attacking probability decreases or in other words cross layer detection scheme should be tried.

- Crossover detection has a problem of using different IDS at each layer which consumes more energy and resources too. So a generalize algorithm for almost all type of attacks should be proposed.

Objectives: following are the key objectives which we have implement in our work:

- The very first objective will be the establishment of WSN network. It can be done by three methods, out of which we will select unsupervised learning for WSN
- Since sensor nodes are resource constrained so we will put a mobile spy in WSN which will take data from every sensor node.
- Detection mechanism has to be deployed on each node which consumes battery of node, rather than we will deploy this only on spy node as it will have the information of every sensor node.
- Voting based detection mechanism will be followed for intruder detection in spy node and results will be shown in form of false alarms in case of different attacks in network.

3. OUR PROPOSED MODEL

In WSN network security and energy consumption are always concern. Security enhancement and reducing the energy consumption algorithm is still in developing stage. The requirement of the algorithm is that there should be tradeoff between these two concerns. In our work we have put a step forward for such type of work. The problem in WSN is categorized in three categories in our work: i) clustering of WSN nodes with cluster head so that minimum energy consumption takes place in data transmission, ii) continuously running a security algorithm and iii) minimization of energy usage. The research map of our work is shown in figure 3.1.

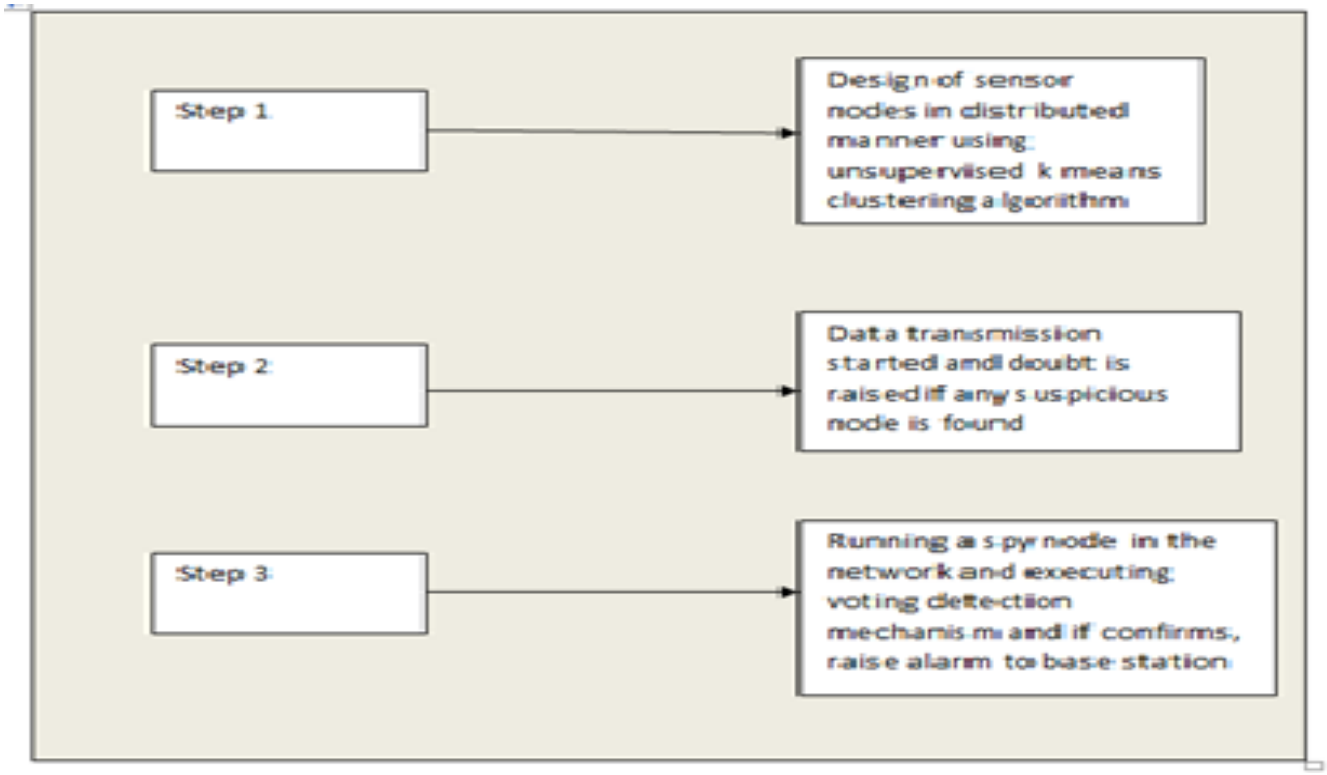


Figure 3.1: Research Map for the proposed Work

Steps for purposed technology:

Step 1: In step first we design the WSN environment by using clustering mechanism. This clustering can be supervised and unsupervised. since nodes placement is a stochastic process, so unsupervised clustering do well. These clustering are done on the basis that nodes are at a minimum distance to cluster head which is chosen on the same criteria so that nodes have to spend minimum energy in transmitting data to base station via cluster head. In our work k-means clustering algorithm is used as unsupervised learning for of clustering of nodes.

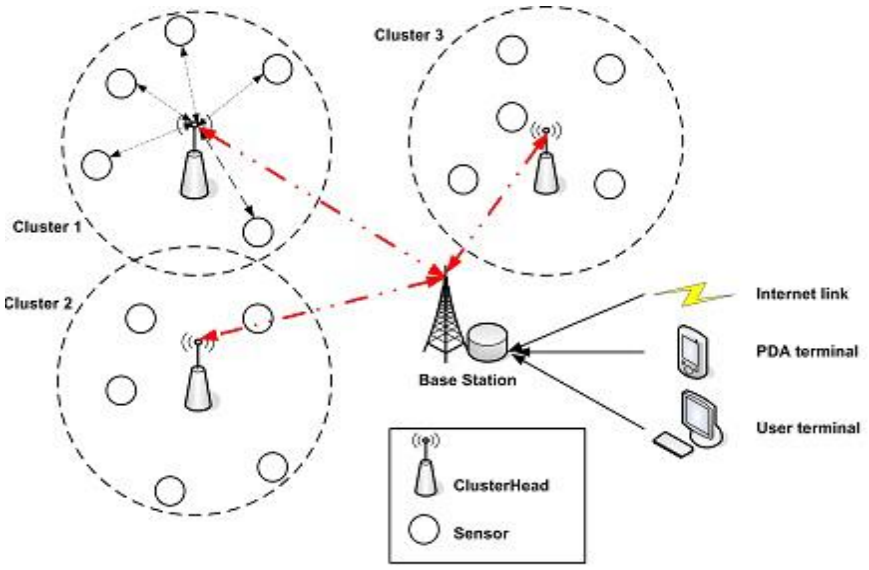


Figure 3.2: Clustered Sensor Network

Step 2: After establishing the WSN nodes in a pattern, security enhancement is the matter to look for. As we know due to open environment WSN is vulnerable o various types of external and internal attack .In all types of attack the sink hole attack in the network layer is worst type attack. Generally our algorithm work for all type of attack but in this paper we show the implementation result mainly for the sink hole attack.

Step 3: In next step our focus mainly on low energy consumption as compared to various schemes purposed by other researcher. So we designed the special type of node i.e. spy node. The detection mechanism is only implemented in spy node instead of all nodes in the network due to resource constrained nature of sensor node. Our detection mechanism is based upon neighboring voting scheme in which which will move throughout the clustered network and collect data from every cluster based on information. In case of detection of malicious node give the alarm.

4. SIMULATION RESULT AND DISCUSSION

We have implementing our purposed work in matlab 2009.The figure shows the main output after executing the code. Each component in diagram are mentioned.

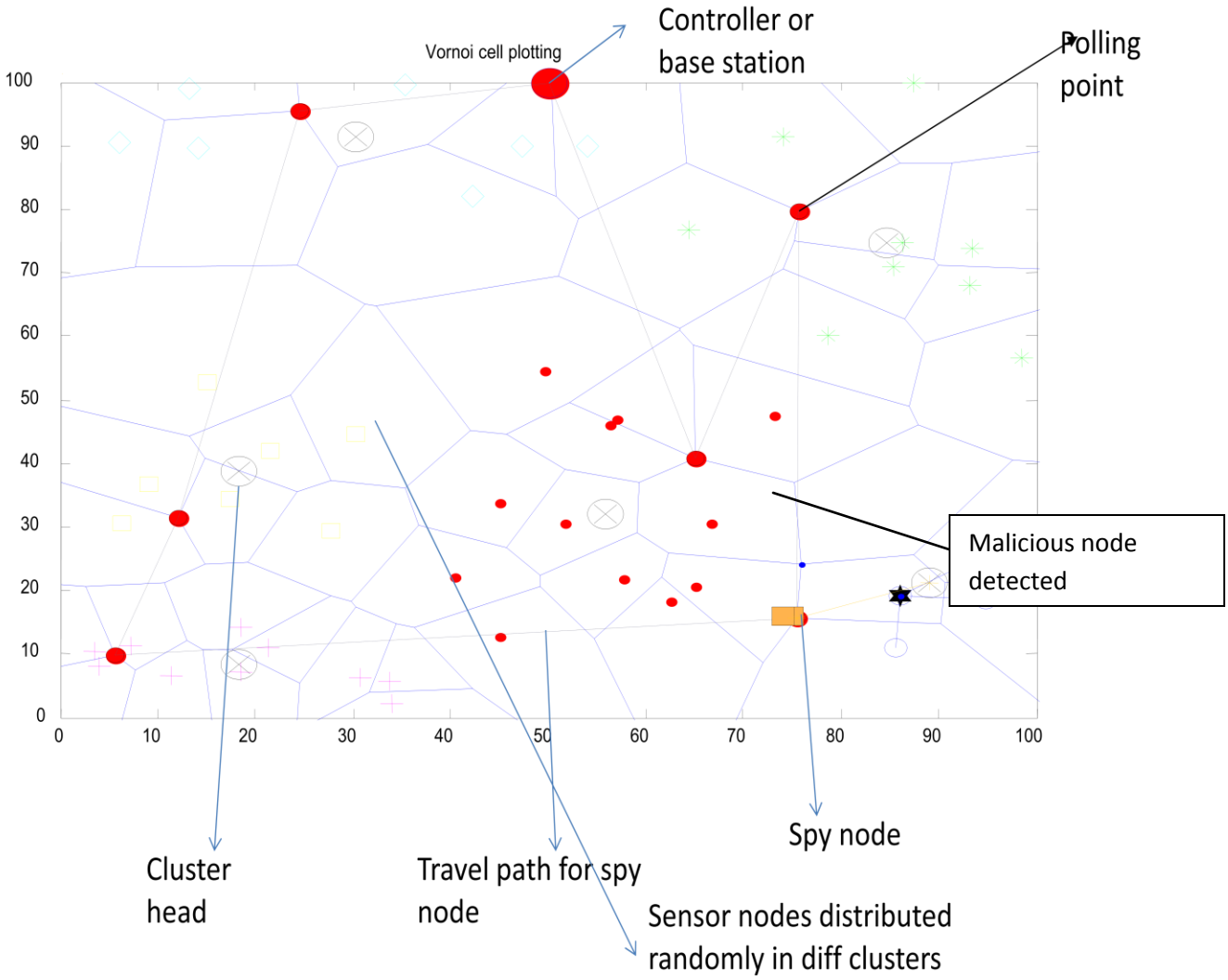


Figure 3.6: Malicious node detection by spy node

The diagram shows the cluster heads in each cluster in this we show the 6 clusters with their nodes and cluster heads. The yellow squares show the spy node which travel throughout the path and stop at polling point i.e. red filling ball and collect data from cluster head and detect malicious node when it is there. The algorithm is executed mainly for sink hole attack in network layer in which later malicious node becomes the sink hole that alter the messages of other nodes which are in the range of its communication. Our purposed algorithm detect the sink hole with good efficiency and low energy consumption as compared to normal algorithm.

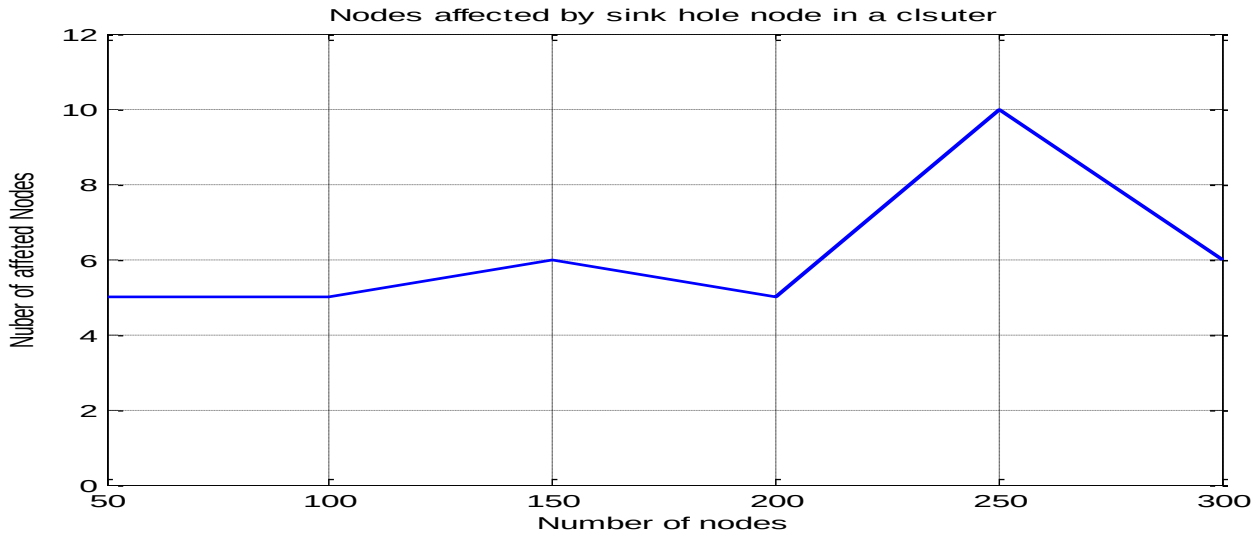


Figure 4.2: Number of affected nodes by sink hole

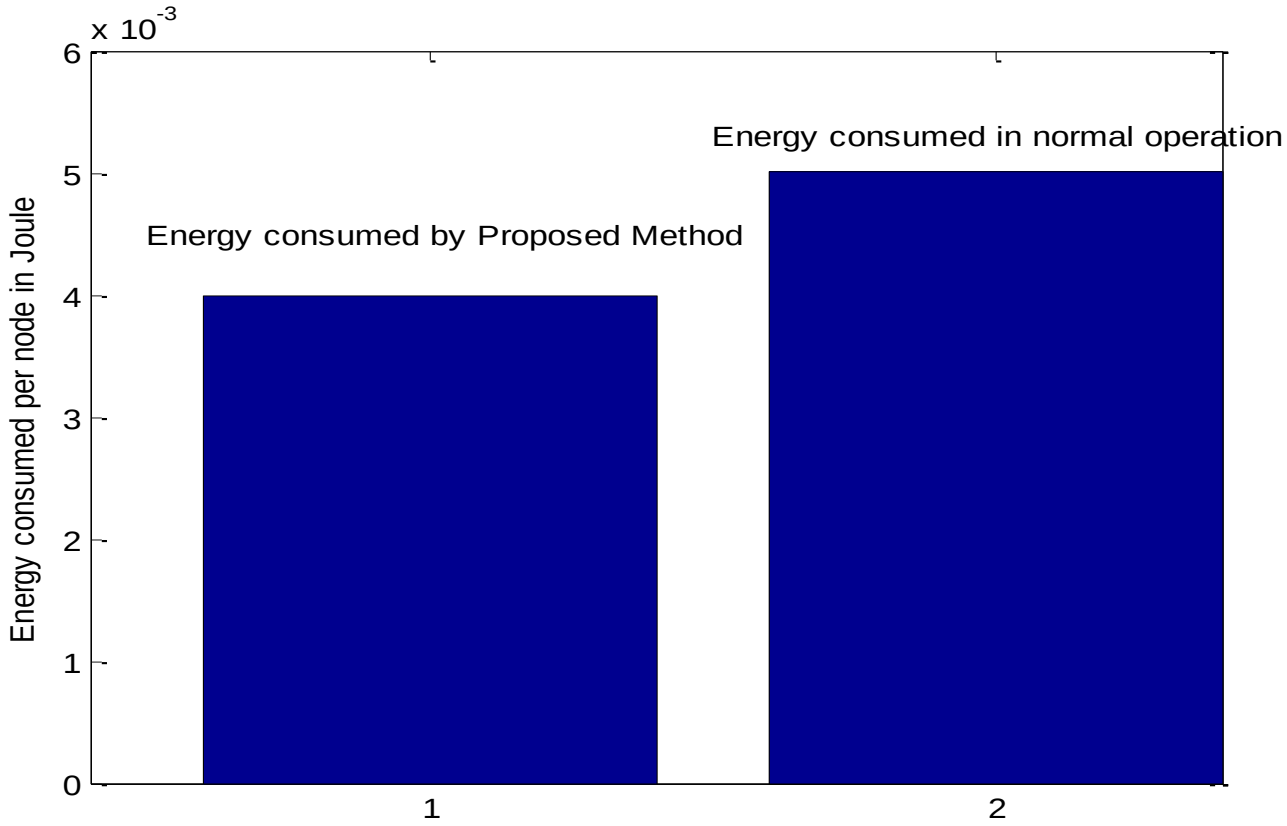
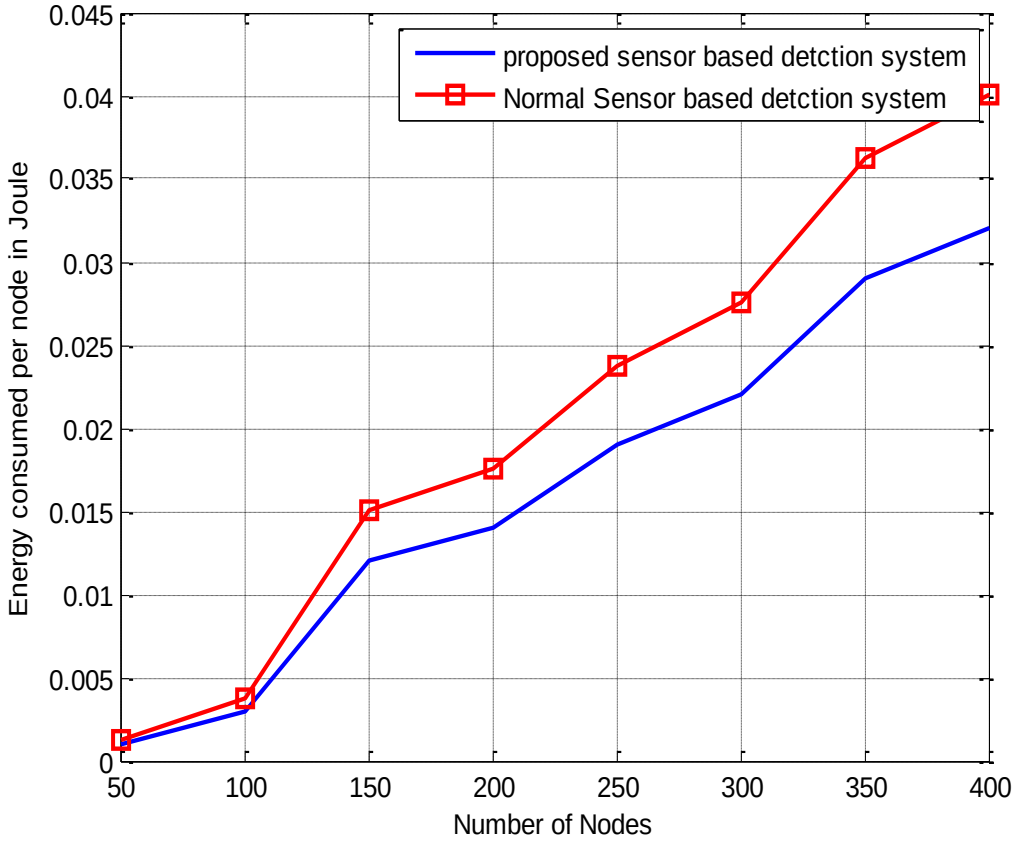


Figure 4.6: energy reduction by proposed method



4.7: Energy consumption for various number of nodes

As nodes are increasing, energy consumption difference is also increasing because of detection mechanism consumption. Since more density of nodes become reason of more nodes affected by intruder. So detection algorithm will be executed by every affected node and this consumes more energy. That's why the difference between both curve in above figure is increasing with density of nodes.

5. CONCLUSION

This work is step forward to development of algorithm which can enhance security and reduce energy consumption at nodes. Since all algorithms can't be avoided by a single universal algorithm, so it makes a clear picture of type of attack to be considered in our work. Sink hole

attack occurs at network layer, so detection mechanism will also execute at that layer. Our mechanism reduces the energy consumption and this difference increases with number of nodes in the network. The detection of intruder is ranging between 0.88-0.92 for various numbers of nodes which is a good factor for true detection.

REFERENCES

[1] G.N. Purohit, "implementation of energy efficient coverage aware routing protocol for wireless sensor network using genetic algorithm."IJFCST, Vol.5, No.1, January 2015.

[2] Umamakeswari Arumugam, "Intrusion Detection Algorithm for Mitigating Sinkhole Attack on LEACH Protocol in Wireless Sensor Networks." Journal of Sensors, Article ID 203814.

[3] K.Muneeswaran, "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.

[4] Joseph Rish Simenthy, "Advanced Intrusion Detection System for Wireless Sensor Networks." International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 3, Special Issue 3, April 2014.

[6] Quazi Mamun, " Anomaly Detection in Wireless Sensor Network." Journal of Networks, vol. 9, no. 11, November 2014.

[7] P.Priyadharshini, "Trust Based Voting Scheme and Optimal Multipath Routing for Intrusion Tolerance in Wireless Sensor Network." IJCSMC, Vol. 3, Issue. 2, February 2014, pg.255 – 260.

[8] Swati Sharma, "Recent trend in Intrusion detection using Fuzzy-Genetic algorithm." International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 5, May 2014.

[9] Chandra Prakash, "A Comparative Study Of Intrusion Detection System For Wireless Sensor Network." IJAFRC, Volume 1, Issue 5, May 2014.

[10] DEEPA S, "Trust Management Schemes For Intrusion Detection Systems -A Survey." International Journal of Advanced Computational Engineering and Networking, Volume-2, Issue-8, Aug.-2014.

[11] Mohammad Abu Alsheikh, "Machine Learning in Wireless Sensor Networks: Algorithms, Strategies, and Applications." IEEE Communications Surveys and Tutorials. 2014.

[12] Sathyabama.B, "Energy Efficient Voting Based Intrusion Detection Techniques in Heterogeneous Wireless Sensor Network." IJCSMC, Vol. 3, Issue. 1, January 2014

