# Attack Detection Algorithm In WSN (Wireless Sensor Network) Using Spy Node

Priyanka, Preeti Prajapati
M.Tech Scholar, N.C. College of Engineering
A.P., N.C. College of Engineering

**Abstract-In the present scenario many advance design of device developed like memory, processors and other communication devices. One of the interested field is WSN(wireless senor network). The WSN has many node in a same network . all the node working on the same time. When nodes running simultaneously the security ratio and energy consideration is the main points of concern. Providing both the task we implement this work. There are some attack which is present in the WSN but sink hole attack is most dangerous to the WSN. It deals with both security and consumption of power. It also provide the path to the other attack. The main purpose of our work to avoid the sink hole attack in WSN. We use spy node for security and energy consumption aspects. A detection algorithm is provided for detection the attacks. The algorithm name is K mean algorithm. Only programming is done in this. The security system will be improved and energy consumption is improved.**

**Keywords- WSN, Spy node, K means algorithm etc.**

## I. INTRODUCTION

A wireless sensor network (WSN) contains a number of gateway (or "base station") that can pass information with a number of sensors nodes via a wireless connection. Information gathered by the node is compressed and sent to the base station directly or if required, it uses other nodes to transfer information to the base station. The information which is transferred , then utilized by base station connection.In Modern trend the WSN is the best network in terms of research concept. The main reason behind that WSN in the various applications in all over the world. The arrangement of small size of sensor nodes the physical phenomena information can be collect easily but through other method it is very difficult to obtain.

## II. CLUSTERING

Clustering has been proposed by researchers to group a number of sensors, usually within a geographic neighborhood, to form a cluster that is managed by a cluster head. A fixed or adaptive approach may be used for cluster maintenance. In a fixed maintenance scheme, cluster membership does not change over time, whereas in adaptive clustering scheme, sensors may change their associations with different clusters over time.

## III. ATTACKS IN WSN

**Jamming:**In this attack the attacker attempts to jam the frequencies of the radio used for communication between the nodes in the network. An adversary may use a few nodes in strategic positions to effectively jam most of the communications inside the network. In essence, an attacker needs only a few nodes in order to disseminate a large network.

**Tampering:** Because of the nature of wireless sensor networks, an adversary could easily get physical access to the sensor nodes. This may enable an attacker to compromise sensor nodes in a DoS like manner.

**Collision:** In This attack a node induces a collision in some small part of a transmitted packet. The packet will then fail the checksum check, because of the changes brought on by the collision, and the receiver node will then ask for a retransmission of the packet.

**Exhaustion:** This attack is one of collision attacks which take them a bit further damage WSNs. A malicious node may conduct a collision attack repeatedly in order to exhaust the power supply of the communicating nodes.

**Misdirection:** In this attack a malicious node that is part of a route can, instead of dropping packets, quite simply send them on a different path which does not exist in a route to the destination. The malicious node may do this for certain packets, or all packets.

**Desynchronisation:** It can disrupt an existing connection between two end points. Adversary transmits a lost packet with bogus sequence numbers or control flags to degrade or prevent the exchange of data.

**Wormhole Attack:** In this attack, a malicious attacker receives packets from one location of a network,

forwards them through the tunnel and releases them into another location. Hence, the attacker is able to send packets, routing information, ACK etc., through a link outside the network to another node somewhere else in the same network. The malicious node can achieve the faith of the neighbor node as a legitimate node [15]. them.

**Sinkhole Attack:** In this attack, a malicious node advertises a zero cost route through itself. If the routing protocol in the network is a "low cost route first" protocol, like distance vector, other nodes will chose this node as an intermediate node in routing paths..

**Sybil Attack:** The concept of Sybil (or multiple-identity) attacks was first proposed by Douceur in P2P networks [35], and it is defined as a single node has multiple identities to disrupt the accordance among the entities and physical devices in a networks..

**Selective Forwarding Attack**: In a simple form of selective forwarding attack, malicious nodes try to stop the packets in the networks by refusing to propagate any further [31]. Another variance of selective forwarding attacks is to delay packets passing through the nodes, creating the confused routing information between sensor nodes.

**Spoofing Attack**:. This can have a serious negative impact on the network performance as well as facilitate many forms of security weaknesses. In this attack, a malicious node is able to create routing loops, wormholes, black holes, partition the network, by spoofing, altering or replaying routing information.

**Hello Flood Attack:** Hello Flood Attack is introduced in. The malicious nodes broadcast hello messages to announce their presence to the neighboring nodes. The node receiving the message assumes that the malicious node is within its range or a neighbor. An attacker with a high powered antenna can convince every node who receives "hello" in the same network which means this node is their neighbor. Hence, the malicious node can deceive other nodes to believe that a normal node is malicious. Nodes at a large distance from the attacker will be sending their messages to an out-of-reach malicious node that can disrupt the network by simply decreasing traffic load and make communications in a state of confusion. This form of attack is specifically designed against routing protocols that are dependent on localized information.

## IV. OBJECTIVE

Keeping problems discussed in mind following will be key objectives which will be tried to achieve 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 nodes distribution as it don't require prior training.
- 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.
- Neighboring Voting 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.

## V. PROPOSED WORK

Our research is categorized in to three main steps.

- The amount of consumption of energy should be very low by bundled of WSN nodes with their head through transmission process.
- A security program always is running.
- Energy usage should be minimize

Cluster provides the more power to node communicate with the other common station. The selection procedure of cluster is called clustering. It may of two types

- Supervised
- Unsupervised

The clustering method which is used in this work is unsupervised because it have many advantages like placement of node is a stochastic process and the nodes are at a small distance to the head so these node required low energy consumption for transmitting the data. It increases the live of node.

The K-means method is used for the clustering of nodes. It use as supervised learning algorithm. It is not very complicated, easy to implement and has simple approaches. The basic concept is that lower distance between cluster head and nodes in same cluster and higher distance of nodes to the other member of nodes of other cluster.

Implementing steps are:

- Specify or generate cluster centers which are called K points.
- Provide each point to the nearest center by find out the distance between data points and centers.
- Evaluate the average value of all data points with respect to cluster then obtain new center points. .
- Then repeat the step 2 with the new points of centers. If some changes in the data points is occur, again repeat step 3 and stop the process

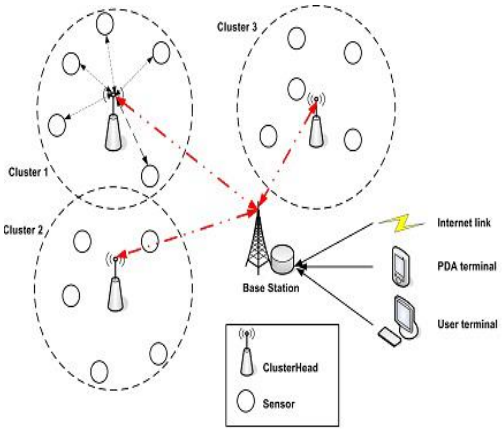


Figure 1: Clustered Sensor Network

make the Voronoi diagram, it divides the region by which all points have same distance from their close source point. This diagram divides the plane in to the regions. It drawn by pairs of points that are very close and drawing a line which is perpendicular to the connecting line. the distance is equal. The diagram shows the Voronoi curve. It will be draw in MAT:AB. Various points are shown which have equal distance to nearby points. this curve identify the position of polling points and spy node is used for running the algorithm and collect the data. All the data on to the base station which is used to locate the cluster head in the area. The polling points location near the cluster head in the limit of spy node. The curve vertex closest to the cluster head so it is in limit with the spy node .But spy node having the ability to communicate so the vertex will be gifted information taking work position and called polling points. The single polling point can give access to more clusters heads. The each cluster having the polling location. The requirement of extra communication equipment depend upon number of cluster accessed at a time. These polling points provide the travel way for spy node.

The wrong information is give to the nodes so network information can be manipulated itself. The sinkhole attack is the network layer attack. The main reason is there are many pattern is used for communication, many nodes are available in the WSN, all the data sends by to nodes in to a single common station. WSNs are particularly vulnerable to sinkhole attacks [11].

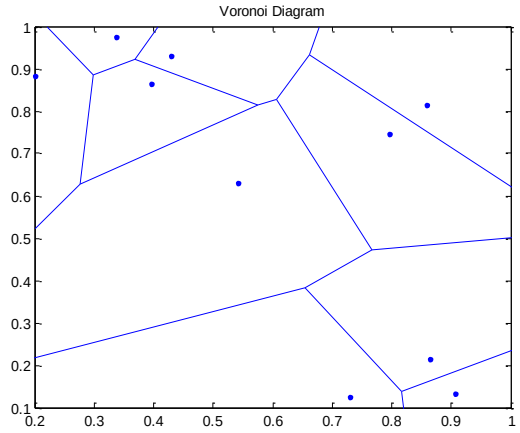


Figure 2: Voronoi diagram

In WSN the sinkhole attack not affected all the nodes present in the area it also affect the closest node to the common station or cluster head. The node which is affected by sink hole has the large power. Using this large power the data can transmit easily to the common station. It also shows the characteristic of node which is close to the cluster head. The spy node follows a feedback path from base station to base station. The algorithm is run on the spy node which found the attack. the cluster can interact with the node directly in clustering process. It is the process which initiate from their cluster head to the common station and then to the sink node. Firstly cluster head receive the data from source node and then cluster head combine both ID ( own and source node) pass to the common station. The common station has all the information of source node and cluster head so they can pass the data with the sink node ID to the cluster head. If some interrupt is present between the nodes then some data or information may be lost in the process.

## VI. RESULTS & DISCUSSION

The position of node in the network provides the security and some energy saving concept. The energy consumption is depend on the position of the node .if the distance is large then energy consumed high if small distance appeared between the node then energy consumption is less. Various methods for nodes placements also employing but we use K means clustering method , The algorithm is used for eliminates the affected node but they have many draw backs like give large number of results and selected on the single data as input like detection based engine data. Suitable number of cluster heads results in minimum energy

consumption of nodes. In our work we have chosen 6 number of cluster heads as shown in figure 3 for 50 nodes.

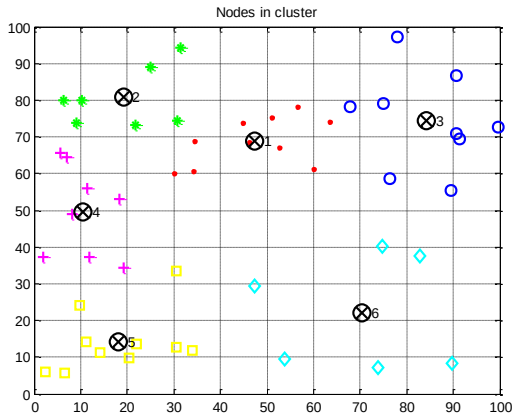


Figure 3: cluster formation in WSN

The representation of cluster separating done by silhouette plot through K means algorithm. It displays the distance of node how they close or far to the other cluster. The ranges are ;

- +1=shows points long distant from cluster.
- 0= shows less distant from the cluster
- -1= shows the wrong cluster selection.

After analyzing the silhouette plot table for various numbers of nodes, cluster head number in our work is set to 6. In the network the nodes are increases, the cluster nodes also increase then more nodes affected by the attacked type node. Many losses are there like information loss or fake information to the network. As shown in the graph number of nodes increases the number of affected nodes.

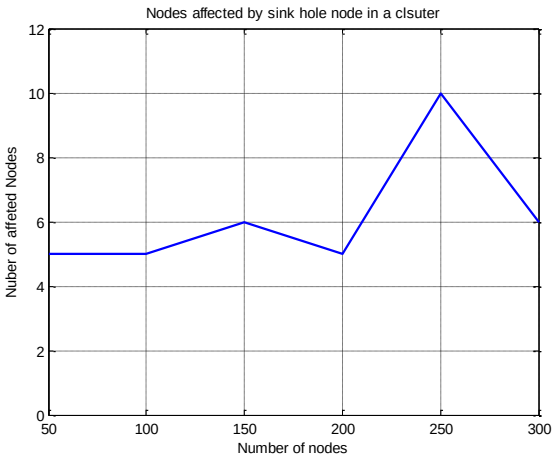


Figure 4.: Number of affected nodes by sink hole

To find the efficiency of the algorithm testing will be done. increase the number of nodes and various iteration has been done. It took two days with 2GB RAM and 1.83 GHz Core2Duo processor for testing of theses much of iterations we have considered. Figure 5 and figure 6 shows the detection of sink hole in the network. Let a single sink hole node which is placed randomly in any cluster every time when new iteration is started. Results have been checked for 50 to 350 nodes and for each number of nodes system is executed from 5 to 30 times, a total of 630 times system have been executed. Figure 5 shows the total number of true detection of Sybil nodes.

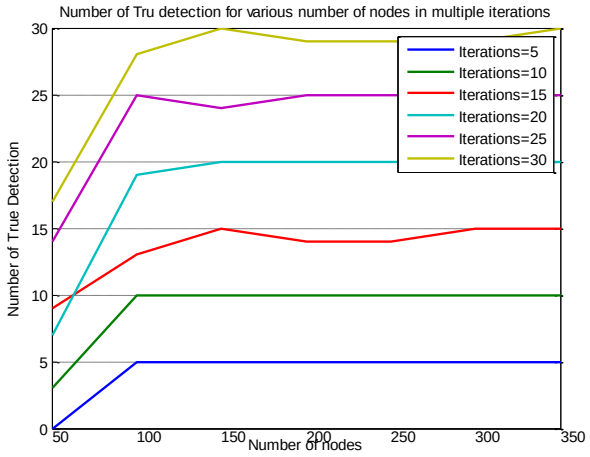


Figure 5: total number of true detection for multiple nodes and iterations

For 50 number of nodes our algorithm skip the detection of sink hole upto a large extent with maximum of 60 % detection in 15 iterations. But as the nodes in the network increased from 50 to 100, a sudden change in locating the sink hole is observed. True detection reached upto 100% in many iterations as shown in figure 6.

For better results than increase the number of nodes regularly.. The average of percentage of true detection is shown in figure 7. It shows that for large number of nodes established in a particular geographical area, sink hole location is in between 0.88-0.92, which is quite impressive.

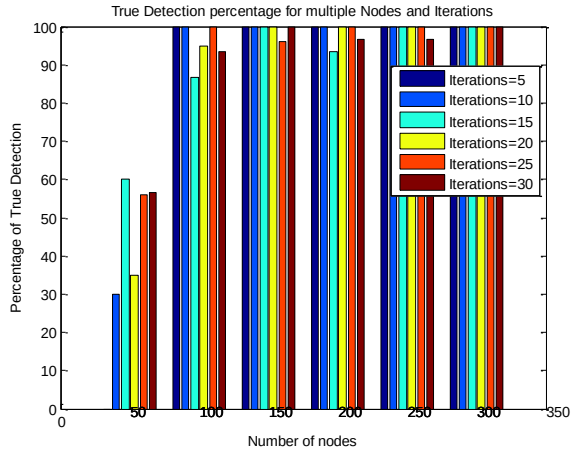


Figure 6: Percentage of true detection for multiple nodes and iterations

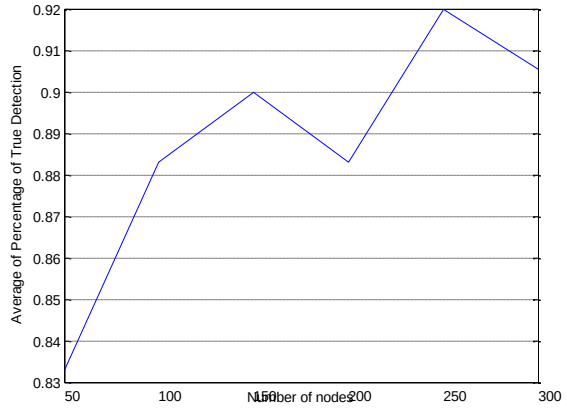


Figure 7: Average number of true detection for multiple iterations

By using the K means algorithm we can provide the security and increase efficiency of the power usage. More power has been saved. The loss of the power is reduced. In this work we use a spy node method. This node is not run in the network it run outside the network and provide less power consumption to the network. The energy consumption is calculated using method discussed in equations 3.2 and 3.3 and initial values used are tabulated in table 4.1. Based on that, the energy consumption graph for 50 nodes is plotted and shown in figure 8 below. It shows that energy consumed by our method is less than previous algorithm. Almost 1 mJ of energy difference is in between two methods. Thus ours is fulfilling dual purpose: security and less energy consumption at nodes. In this energy calculation, only nodes which are affected by malicious nodes are considered as rest nodes are not taking part in transmission in our case. A comparison of energy consumption for multiple sensor nodes is show in figure 9. That figure also proves that although total energy consumption increases with increase in number of nodes, yet it is less than normal operation

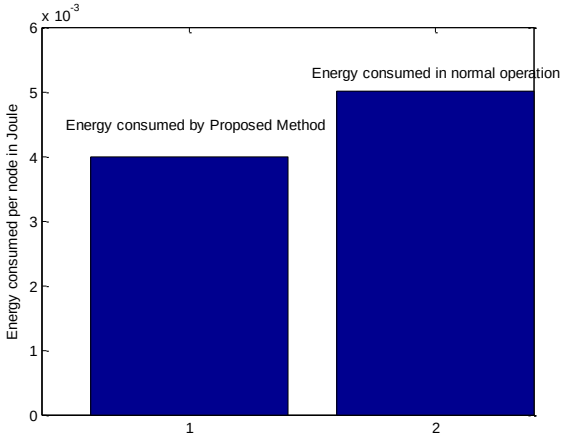


Figure 8: energy reduction by proposed method

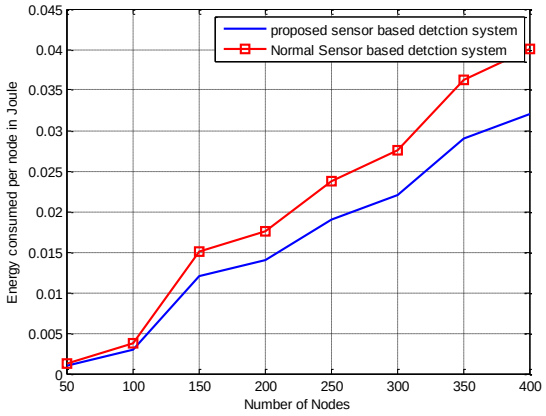


Figure 9: Energy consumption for various number of nodes

figure shows the consumption of energy when nodes are increased. The reason behind it detection process. The node with greater density mostly affected by the attack. So the detection process through that node consumes large energy.

## VII. CONCLUSION

we implement an algorithm which provides security and less energy consumption to the WSN. In a network there are some nodes present. The node has individual densities. In case of wireless sensor network there are various nodes and some attack affected the node randomly. If a node has high density than attack is occur on that node. The affect of attack increases the consumption of power. There are many types of attacks present in the network but sink hole attack mostly affected the node. The sink hole attack increases the energy consumption. If we implement an algorithm of

detection on that node some losses increases more. So we use a spy node , it is not the node of the network it provides running to the implement algorithm . the energy consumption is reduced and security concept improved. It has been proved that proposed algorithm is also performing well for security too. 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] Mahdi Shahedi, "A Trust Based Routing Protocol for Mitigation of Sinkhole Attacks in Wireless Sensor Networks." International Journal of Information and Education Technology, Vol. 5, No. 7, July 2015.
[4] 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.
[5] 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, pg. 374 – 380.
[13] K.Kumaresan, " Weighted Voting based Trust Management for Intrusion Tolerance in Heterogeneous Wireless Sensor Networks." IJAFRC, Volume 3, Issue 6, Nov 2014.
[14] Sneha Dhage, " Intrusion Detection & Fault Tolerance in Heterogeneous Wireless Sensor Network: A Survey." International Journal of Scientific and Research Publications, Volume 4, Issue 2, February 2014.
[15] Jaime Lloret, "Intrusion Detection Algorithm Based on Neighbor Information Against Sinkhole Attack inWireless Sensor Networks." The Computer Journal Advance Access published May 13, 2014.
[16] Suhasini Komara, " Sinkhole Attack Detection In Hierarchical Sensor Networks." International Journal of Scientific & Engineering Research, Volume 5, Issue 9, September-2014.
[17] Junaid Ahsenali Chaudhry, "Sinkhole Vulnerabilities in Wireless Sensor Networks." International Journal of Security and Its Applications Vol.8, No.1 (2014), pp.401-410.
[18] Nabil Ali Alrajeh, "Secure Ant-Based Routing Protocol for Wireless Sensor Network." International Journal of Distributed Sensor Networks ,Volume 2013, Article ID 326295, 9 pages.
[19] Udaya Suriya Rajkumar, "A Leader Based Monitoring Approach For Sinkhole Attack In Wireless Sensor Network." Journal of Computer Science 9 (9): 1106-1116, 2013.
[20] R˘azvan Rughinis, "Adaptive Trust Management Protocol based on Intrusion Detection forWireless Sensor Networks." International Journal of Scientific & Engineering Research, Volume 1, Issue 9, September-2012.
[21] Sibaram Khara, "K-Means Clustering In Wireless Sensor Networks." Fourth International Conference on Computational Intelligence and Communication Networks, 2012.
[22] Shio Kumar Singh, "Intrusion Detection Based Security Solution for Cluster-Based Wireless Sensor Networks." International Journal of Advanced Science and Technology Vol. 30, May, 2011.
[23] Ioannis Krontiris, "Cooperative Intrusion Detection in Wireless Sensor Networks." International Journal of Distributed Sensor Networks, 2011.
[25] Md. Safiqul Islam, "Anomaly Intrusion Detection System in Wireless Sensor Networks: Security Threats and Existing Approaches." International Journal of Advanced Science and Technology Vol. 36, November, 2011.
[26] C. Kolias, "Swarm intelligence in intrusion detection: A survey." IJAFRC, Volume 2 Issue3, Nov 2011.
[27] Michael Krishnan, "Intrusion Detection in Wireless Sensor Networks." ACM SENSYS, November 2010.
[28] Marcelo H.T. Martins, "Decentralized Intrusion Detection in Wireless Sensor Networks." Q2SWinet'05, October 13, 2010.
[29] Ioannis Krontiris, "Intrusion Detection of Sinkhole Attacks in Wireless Sensor Networks."International Journal of Advanced Science and Technology Vol. 36, November, 2009.
[30] D. Sheela, "A Recent Technique to Detect Sink Hole Attacks in WSN." Journal of Computer Science 9 (9): 1106-1116, 2005.
[32] K. Sharma and M. K. Ghose, "Wireless Sensor Networks: An Overview on its Security Threats," IJCA, Special Issue on "Mobile Ad-hoc Networks" MANETs; CSE Department, vol. 1, no. 1, pp. 42–45, 2010.
[33] H. K. D. Sarma and A. Kar, "Security Threats in Wireless Sensor Networks," in Carnahan Conferences Security Technology, Proceedings 2006 40th Annual IEEE International, Oct., pp. 243–251.
[34] H. Ghamgin, M. S. Akhgar, and M. T. Jafari, "Attacks in Wireless Sensor Network," vol. 5, no. 7, pp. 954–960, 2011.
[35] Padmalaya Nayak, V. Bhavani," Impact of Black Hole and Sink Hole Attacks on Routing Protocols for WSN" International Journal of Computer Applications (0975 – 8887) Volume 116 – No. 4, April 2015
[36] M. Corporation, "Data sheet Tmote sky." Moteiv Corporation, 13-Nov-2006.
[37] B. Cross, "MICA 2: Wireless Measurement System." Crossbow technologiey, Inc, 2009.