INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

IDS IN WSNs-BASED ON SPY NODE AND BALLOT SCHEME

Nidhi Kundu[1], Navneet Verma[2]

[1,2]Geeta Engineering College
Naultha, Panipat, Haryana (132103), India
[1]kundu.nidhi1990@gmail.com, [2]navneet.cse@geeta.edu.in

Abstract*: Due to the distributed nature, multi-hope communications and their deployment in remote areas, WSNs are susceptible to numerous security attacks that can adversely affect performance. Therefore, to ensure the proper functionality of WSNs, security is the foremost and important concern in almost all wireless sensor networking scenarios. WSN mechanisms cannot presently ensure that an intrusion will not occur. For example, using a compromised node, an adversary could do an attack acting as a correct node of the network to acquire all the information. Such attacks are called as internal attacks. Therefore, it is necessary to protect the wireless sensor network from internal attacks, which is the purpose of this paper. Algorithm for transport layer attack has been developed in this paper which also focuses on minimum energy consumption. We have tested the algorithm for sink hole attack mainly using voting scheme but it can also works for other attacks like worm hole attack, black hole attack.*
Keywords*:-WSN, Clustering, K-means algorithm, sinkhole attack, Spy node.*

1. INTRODUCTION

Efficient design and implementation of wireless sensor networks has become a hot area of research in recent years, due to the vast potential of sensor networks to enable applications that connect the physical world to the virtual world. By networking large numbers of tiny sensor nodes, it is possible to obtain data about physical phenomena that was difficult or impossible to obtain in more conventional ways. In the coming years, as advances in micro-fabrication technology allow the cost of manufacturing sensor nodes to continue to drop, increasing deployments of wireless sensor networks are expected, with the networks eventually growing to large numbers of nodes. Potential applications for such large-scale wireless sensor networks exist in a variety of fields, including medical monitoring, environmental monitoring, surveillance, home security, military operations, and industrial machine monitoring. When designing network protocols for wireless sensor networks, several factors should be considered. First and foremost, because of the scarce energy resources, routing decisions should be guided by some awareness of the energy resources in the network. If a sensor network is well connected (i.e. better than is required to provide communication paths), topology control services should be used in conjunction with the normal routing protocols. Simple sensor nodes are usually not well physically protected because they are cheap and are always deployed in open or even in hostile environments where they can be easily captured and compromised. That is why it has become a challenging task to secure WSN.

As WSN suffers from various attacks by anomaly nodes. These nodes are stated as intruders which can alter the message passed to base station. 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 literature survey are listed -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. Keeping problems discussed in mind 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. 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.

2. LITERATURE REVIEW

Intrusion detection is an important aspect in the large domain of computer network security. Main focus on Intrusion Detection System[4] offering a new game theoretic-approach and focus only on the anomaly based intrusion detection system[6]. New intrusion detection system based on cross layer interaction between the network, Mac and physical layers[10].Also an efficient MAC address based intruder tracking system[8], Indeed we have addressed the problem of intrusion detection in a different way in which the concept of cross layer is widely used leading to the birth of a new type of IDS. We have experimentally evaluated our system using the NS simulator to demonstrate its effectiveness in detecting different types of attacks at multiple layers of the OSI model. Some intusion system is anomaly based many authors worked on such system**.** In Intrusion detection system to save energy many clustering algorithms used like K-means algorithm. An both centralized and distributed k-means clustering algorithm approach used in network simulator[9][31].

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

k-means is a prototype based algorithm that alternates between two major steps, assigning observations to clusters and computing cluster centers until a stopping criterion is satisfied. An Intrusion Detection System (IDS) mechanism to detect the intruder in the network which uses Low Energy Adaptive Clustering Hierarchy (LEACH) protocol for its routing operation [30]. An adaptive secure routing protocol which is based on bio inspired Mechanism of Several efficient routing protocols are proposed for specific scenarios to achieve particular objectives in WSN [13]. However, such networks have many limitations such as low data rates and security threats. It uses distributed ant-based methodology to select two optimal paths keeping in view route security. Simulation results show that our routing protocol can perform better in many scenarios. An efficient MAC address based intruder tracking system has been developed for early intruder detection and its prevention [8]. Wireless sensor network (WSN) is an emerging technology that shows great promise for various applications both for mass public and military. A Voronoi diagram based network architecture, which deploys mobile data collectors (MDCs), ensures the compatibility of the anomaly detection model for the resource constrained WSNs, and warrants data integrity between the MDCs [25] and the LNs. A parameter and trust factor based secure communication framework and design a trust management system for wireless sensor networks[28].Wireless network system susceptible to lot of attacks out of this sink hole attack[15][16] is the most dangerous as it give path for other attacks too. A scheme to defend against sink hole attacks[1][2] using mobile agents and Leader Based Intrusion Detection System (LBIDS) in order to provide a complete solution to detect and avoid [14][12] sinkhole attack. **T**he Adaptive Trust Management Protocol (ATMP), that adjusts trust and reputation based on the behavior of sensor nodes [29][11]. Some considered multidimensional trust attributes derived from communication and social networks to evaluate the overall trust of a sensor node [17]. The weighted vote primarily based Trust Management theme to boost the performance of intrusion tolerance in HWSN [18][24]. An extensive literature review of machine learning methods that were used to address common issues in wireless sensor networks [20] (WSNs). Some cooperative [7] and advanced[26] methods of Intrusion detection was also proposed. Swarm Intelligence (SI), a relatively new bio inspired family of methods, seeks inspiration in the behavior of swarms of insects or other animals. After applied in other fields with success SI started to gather the interest of researchers working in the field of intrusion detection[5].

3. PROPOSED WORK

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.

Step 1: In WSN each node can communicate with other freely, but if let it happen then no particular routing algorithm will be effective and since every node has to transmit data to base station which is placed at a very far distance from many of nodes and nodes are always equipped with power constraint battery sources, so in transmitting messages to a far distance will drain out their battery very fast. To avoid this many nodes collectively choose a head amongst them which is near to many of nodes and have enough power to communicate with base station, irrelevant to distance. That node head selection is called clustering. 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. It's a kind of hierarchy, which lets nodes to live more. Our work used unsupervised learning methodology. In clustering algorithm nodes doesn't communicate directly with sink node. They have to pass the collected data to the cluster head. Cluster head will aggregate the data, received from cluster nodes and transmits it to the base station. Thus minimizes the energy consumption and number of messages communicated to base station. Also number of active nodes in communication is reduced. In our work k-means clustering algorithm is used as unsupervised learning for of clustering of nodes. Steps for implementing the k means clustering are:

- Arbitrarily generate k points (cluster centers),k being the number of clusters desired.
- Calculate the distance between each of the data points to each of the centers, and assign each point to the closest center.
- Calculate the new cluster center by calculating the mean value of all data points in the respective cluster.
- With the new centers, repeat step 2. If the assignment of cluster for the data points changes, repeat step 3 else stop the process.

The distance between the data points is calculated using Euclidean distance.

Step 2: After establishing the WSN nodes in a pattern, security enhancement is the matter to look for. Various attacks on WSN have been identified till now like Sybil attack, black hole attack. Amongst all, sink hole attack is more dangerous as it can alter the data and opens a path to other attacks too. For detection of sink hole attack various methods have been suggested previously but none of them is full proof and if anyone is then that forgets the energy consumption. But in our work we kept a win to win situation in between them. In many detection algorithms, nodes are responsible to run algorithm on their part which consumes energy. But if this detection technique is not the responsibility of nodes then battery power of nodes can be saved up-to an extent. To keep this in mind we used the concept of a spy node which will keep running through

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

whole network, connecting with base station. Since it will start from base station and end at base station so battery requirement will not be constraint for it. In the geographical area many polling points will be decided on which spy node will collect the data from nearby cluster head and detection algorithm will be run on the spy node, not in the node. It thus saves energy of node. For this purpose all geographical area is divided by voronoi diagram and polling point are located on the basis of that.

Step2.1 Voronoi diagram divides the region in such a manner that all points on the lines in the diagram are equidistant to the nearest two (or more) source points. It's a diagram created by taking pairs of points that are close together and drawing a line that is equidistant between them and perpendicular to the line connecting them.

Step 2.2: voronoi vertices will locate the position of polling point where spy node will collect the information and run the detection algorithm. Base station has all information about the position of cluster head in geographical area and it would be quite easier to setup the polling location near cluster head which is in range of spy node. Since spy node is also having a range to communicate so the voronoi vertex nearest to cluster head which comes in the range of spy node from that vertex will be awarded data collecting work position and called polling point. In our work we have assigned each polling location for each cluster. These polling points will make a travel path for spy node as shown in figure 1 below, designed in MATLAB during our work. Blue color lines show the voronoi edges and red dots shows polling point location where spy node will collect data form cluster head. Dotted lines show the path of spy node.

Step 2.3: In clustering nodes in cluster can't talk to other cluster nodes directly. They have to follow a hierarchy which starts from their cluster head to base station and then to respective cluster head of sink node.

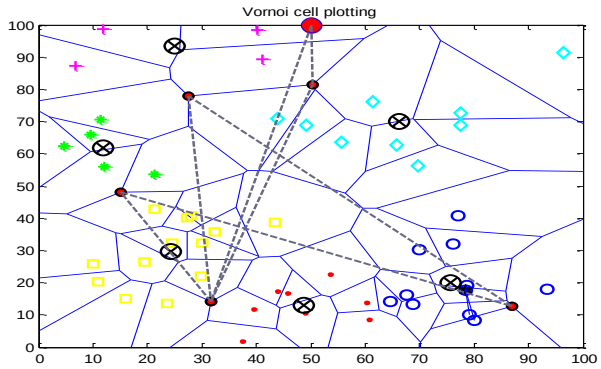

Figure 1: Voroni edges and polling point location along with spy node path

Each source node transmits its data to cluster head and then cluster head add source node's ID and own ID with the data and send it to base station. Base station has all information about tall nodes and cluster head to which they are associated, so it will route the message along with the sink node ID to respective cluster head. But if any node is affected by intruder then the data transferred to base station either altered or lost in between. In a sinkhole attack an intruder compromises an existing node or introduces a counterfeit node inside the network and uses it to launch an attack. The attacker node tries to attract all the traffic from neighboring nodes based on the routing metric used in the routing protocol. Sinkhole attacks are a form of network layer attack where the compromised node sends fake routing information to its neighbors to attract network traffic to itself. Based on the communication flow in the WSN the sinkhole does not need to target all the nodes in the network but only needs to target nodes close to the base station or cluster head if it occurs within a cluster. It reflects the identity of a node which is just next to cluster head or base station to other nodes. In consequence of which nodes treat it single hope away from cluster head and transfers the data to sink hole node which is altered by that and further sent to cluster head and then sink hole followed by hierarchy. In our work sink hole is chosen randomly in any cluster and it create illusion of one hope away identity to others and alter their data as shown in figure 2.

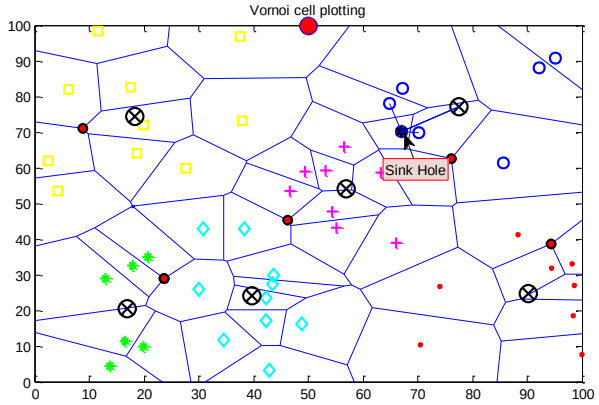

Figure 2: Sink hole affecting other nodes in range

We have considered the energy of sink hole same as other nodes. Number of nodes affected by sink hole depends upon the density of nodes. More will be nodes in a cluster more nodes will be affected.

Step 2.4: because of serious attacks by sink hole the detection and removal from the network is necessary. Base station has the authority to allow access to any node in the network or can remove any node too. So once malicious node is detected, base station will remove that. Our study used the voting based algorithm to detect the intruder. Many algorithms have been considered to detect this network layer attack but many of them run detection engine based on data of single node that may result in errorneous result. If neighboring nodes assistance is also included in the detection engine then more confidence on detection mechanism can be built. For this purpose we used voting based algorithm, if majority of nodes voted against any node then that node will be considered as malicious node. This process executes in two steps:

- When any node communicates with malicious node then a doubt will be raised about the malicious node.
- If major number of communicating nodes raised doubt about the particular node then that will be confirmed as intruder and an alarm will be raised to base station about the identity of that node and base station remove that node form the network.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

In our work we have taken as two nodes' doubts as threshold to elect the particular node as malicious node.

Step 3: energy is consumed in transmission and reception of sensor node. If intruder detection mechanism is run on sensor node then that also consumes energy and since node is always energy constrained, so it would be better if detection mechanism is executed on another node which doesn't contribute in making network. So to avoid running detection mechanism on nodes, a spy node is used which will keep moving in the network and collect data form cluster heads at pre allocated polling points. The detection mechanism will be run on spy node. it collects data from cluster head and check whether any doubt is raised or not, if raised then it will follow voting mechanism and raises alarm to base station. The travel path for spy node is already designed in previous step. In WSN when any node transmits data then it also add its ID along with destination ID and data. When sink hole gets the data and transmits it to head after altering it, it has to add its ID also. This all table of data sent from nodes to head is passed to spy node which can easily check the last hope node ID. If multiple nodes send data through compromised node to cluster head then in their routing table malicious node ID will be in last hope node ID to cluster head. If the occurrence of this same ID is more than two times, then that node is confirmed as malicious node as in figure 3 and base station removes that from network.

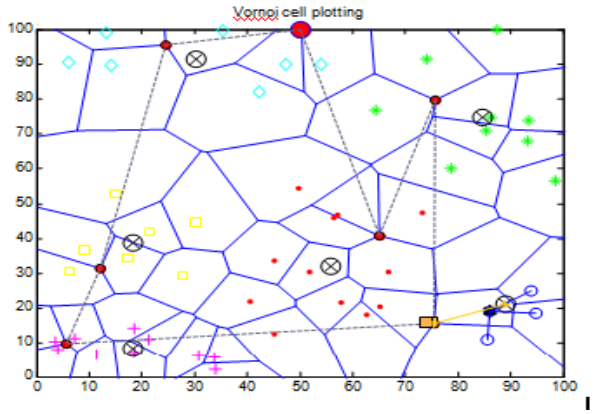

Figure 3: Malicious node detection by spy node

4. RESULT AND DISSCUSSION

In the paper, work for the detection of sink hole node is done and on the criteria of number of true detections, effectiveness of algorithm is judged. Every intruder detection algorithm suffers from the limited battery resources on sensor nodes. So a tradeoff between security and energy efficiency must be in developed algorithm. In our work this is done by moving a spy node in the network. We have considered the energy constraint and calculated energy in each transmission and reception of message through a sensor node who takes part in communication. Parameters considered in this paper are tabulated in table 1 fetched form paper of [8]. The nodes placement in network affects the security and energy consumption. We picked k means clustering algorithm for nodes placement. In this, cluster heads are selected randomly amongst nodes and on the basis of minimum distance to head and maximum to others, rest nodes are assigned to these clusters for its communication. It lets the less requirement of energy in communication. In our work we have chosen 6 number of cluster head.

Table 1: Parameters' values considered for the simulation

Nodes	[50 100 150 200 250 300 350]
Geographical area	100*100 square meter
Energy consumed in reception	50 nJ
Energy consumed in Transmission	50 nJ
Data packet length	10Kb
Energy consumed in detection process	5nJ*
Packet size for sending alarm to base station	5Kb
Transmission range of sensor nodes	10 meter
Number of iteartions	[5,10,15,20,25,30]

To get an idea of how well-separated the resulting clusters are, a silhouette plot using the cluster indices output from kmeans can be drwan. The silhouette plot displays a measure of how close each point in one cluster is to points in the neighboring clusters. This measure ranges from +1, indicating points that are very distant from neighboring clusters, through 0, indicating points that are not distinctly in one cluster or another, to -1, indicating points that are probably assigned to the wrong cluster. Silhouette plot for above cluster and different number of cluster heads is shown in figure 4 and 5. Below figure shows, for some cluster heads silhouette plot has values in negative range too, which shows some nodes are assigned to wrong cluster heads. This plot judges the selection of number of cluster heads. After analyzing it for various numbers of nodes, cluster head number in our work is set to 6.

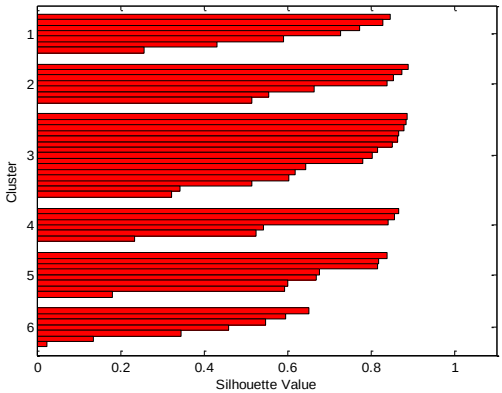

Figure 4: Sillhouette Plot for 6 number of cluster heads

The number of affected nodes with increase in number of nodes. To prove the efficiency of the algorithm, testing for varying number of nodes and multiple iterations 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. We have considered 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

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

executed from 5 to 30 times, a total of 630 times system have been executed.

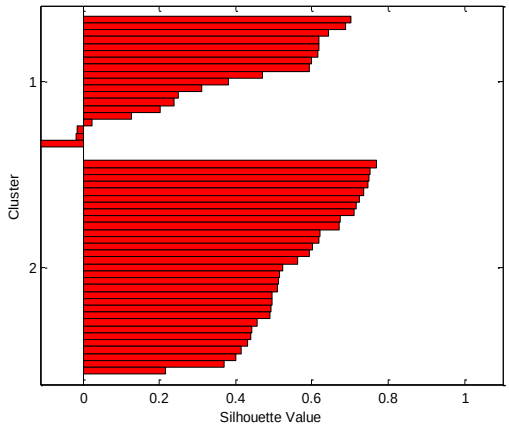

Figure 5: Sillhouette Plot for 2 number of cluster heads

For 50 number of nodes our algorithm skip the detection of sink hole up-to a large extent with maximum of 60 % detection in 15 iterations.

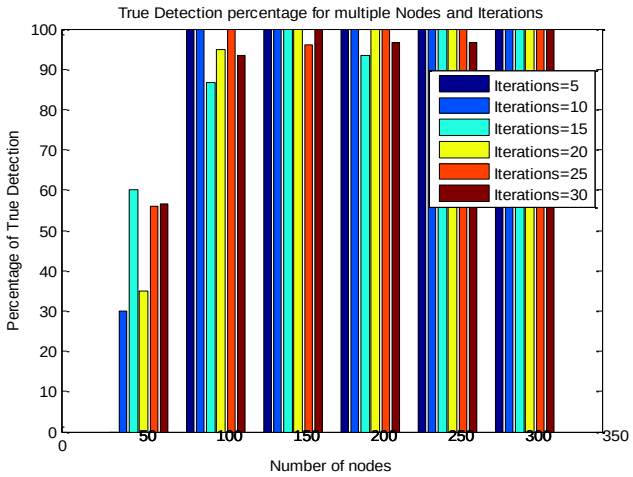

Figure 6: Percentage of true detection for multiple nodes and iterations

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 up to 100% in many iterations as shown in above figure 6. For further increase in number of nodes, promising results are visible. 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.

Till now security part of our algorithm has been discussed, our algorithm reduces the energy consumption along with enhanced security. For this a spy node runs in the network and intruder detection mechanism runs on spy node. Based on that, the energy consumption graph for 50 nodes is plotted, it clearly depicts that energy consumed by our method is less than previous algorithm in figure 7. 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 8.

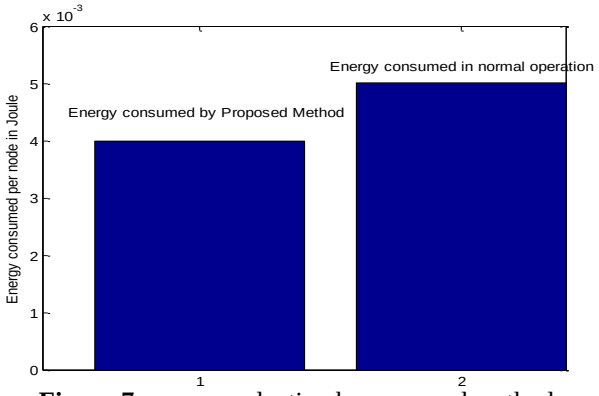

Figure 7: energy reduction by proposed method

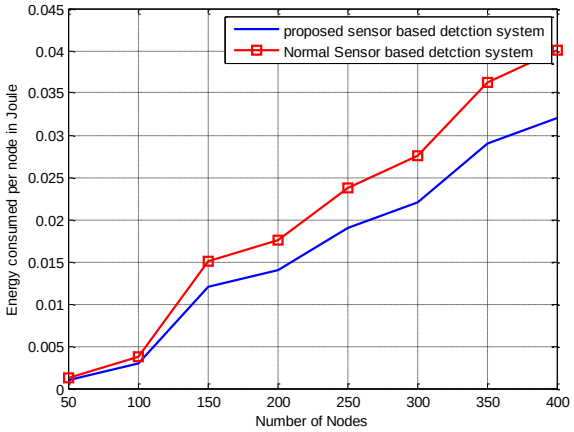

Figure 8: Energy consumption for various no. of nodes

5. CONCLUSION AND FUTURE WORK

WSNs are an emerging technology for monitoring environment. The resource constraint sensor nodes are more vulnerable to attacks in wsn as the nodes are deployed in open environment.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. 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. We have considered single intruder randomly placed in any cluster. In future the cost of moving the spy vehicle in the network and environment for sending message to base station can be considered.

REFERENCES

[1] D. Sheela, "A Recent Technique to Detect Sink Hole Attacks in WSN." Journal of Computer Science 9 (9): 1106-1116, 2005.

[2] Ioannis Krontiris, "Intrusion Detection of Sinkhole Attacks in Wireless Sensor Networks."International Journal of Advanced Science and Technology Vol.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

36, November, 2009.

[3] Marcelo H.T. Martins, "Decentralized Intrusion Detection in Wireless Sensor Networks." Q2SWinet'05, October 13, 2010.

[4] Michael Krishnan, "Intrusion Detection in Wireless Sensor Networks." ACM SENSYS, November 2010.

[5] C. Kolias, "Swarm intelligence in intrusion detection: A survey." IJAFRC, Volume 2 Issue3, Nov 2011.

[6] 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.

[7] Ioannis Krontiris, "Cooperative Intrusion Detection in Wireless Sensor Networks." International Journal of Distributed Sensor Networks, 2011.

[8] 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.

[9] Sibaram Khara, "K-Means Clustering In Wireless Sensor Networks." Fourth International Conference on Computational Intelligence and Communication Networks, 2012.

[10] Djallel Eddine Boubiche, "Cross Layer Intrusion Detection System Wireless Sensor Network." International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012.

[11] Razvan Rughinis, "Adaptive Trust Management Protocol based on Intrusion Detection forWireless Sensor Networks." International Journal of Scientific & Engineering Research, Volume 1, Issue 9, September-2012.

[12] Udaya Suriya Rajkumar, "A Leader Based Monitoring Approach For Sinkhole Attack In Wireless Sensor Network." Journal of Computer Science 9 (9): 1106-1116, 2013.

[13] 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.

[14] Junaid Ahsenali Chaudhry, "Sinkhole Vulnerabilities in Wireless Sensor Networks." International Journal of Security and Its Applications Vol.8, No.1 (2014), pp.401-410.

[15] Suhasini Komara, "Sinkhole Attack Detection In Hierarchical Sensor Networks." International Journal of Scientific & Engineering Research, Volume 5, Issue 9, September-2014.

[16] Jaime Lloret, "Intrusion Detection Algorithm Based on Neighbor Information Against Sinkhole Attack in Wireless Sensor Networks." The Computer Journal Advance Access published May 13, 2014.

[17] 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.

[18] K. Kumaresan, "Weighted Voting based Trust Management for Intrusion Tolerance in Heterogeneous Wireless Sensor Networks." IJAFRC, Volume 3, Issue 6, Nov 2014.

[19] Sathyabama. B, "Energy Efficient Voting Based Intrusion Detection Techniques in Heterogeneous Wireless Sensor Network." IJCSMC, Vol. 3, Issue. 1, January 2014, pg. 374 – 380.

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

[21] 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.

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

[23] 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.

[24] 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.

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

[26] 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.

[27] 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.

[28] Geetha V., "A Distributed Trust Based Secure Communication Framework for Wireless Sensor Network." Scientific Research Publishing Inc., August 2014.

[29] 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.

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

[31] 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.