finally the performance is evaluated by determining the detection rate and energy overhead in IDS nodes. The dynamic IDS models are better when compared with static IDS and it helps to increase the lifetime of network.

4. Proposed Methodology

The proposed approach uses the hybrid intrusion detection system in the clustered network. In each cluster, a cluster-head is selected based on adaptive leader election. The IDS agents are trained well about the various attacks. The mobile sink is added as an intermediate between the cluster head and the base station. The mobile sink is dynamic and gathers the data from cluster head and transmits it to the base station. If any intruder attacks the system, the IDS agent classifies it. The following are the concepts used in the proposed method to enhance the energy of the CH node thereby reducing the consumption of energy in the intrusion detection framework.

In the network zone, an extra node is added which in moving state that gathers the data from each of the cluster-head and transmits to the base station. In each cluster, there are a) Sensor Nodes b) IDS Agents c) Cluster-Head. The work of IDS (Intrusion Detection System) is to train the agents/nodes about the various kinds of attacks. The hybrid intrusion detection is used here that combines the advantage of both signature based detection and anomaly based detection. The signature based detection has a set of predefined rules or behavior that helps to identify the attack. The anomaly based detection uses SVM-based detection to classify the type of attack. The main task of the proposed system is to identify the type of intruder, secure cluster-head from being a selfish node, to select the best cluster-head based on adaptive algorithm and to reduce the false positive rates in the network. The proposed network topology is shown in the following figure.

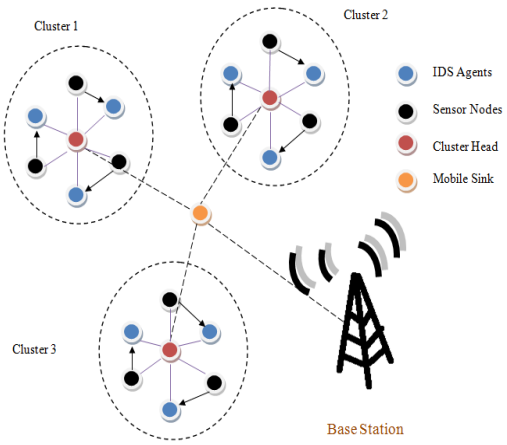

Figure 2: Proposed CWSN topology

A. Adding mobile sink to the network

In general CWSN, the CH gathers the data from all the nodes in the particular cluster and then sends it to the Base Station (BS). The CH is also one of the sensor nodes and hence the energy of the cluster-head (CH) used to gather the data should be less. The energy of the sensor nodes is one of the main criteria that should be noted. If the nodes are out of energy then the nodes are dead. Whenever the nodes are not in use, the sensor nodes must be put in sleep mode to save energy. In order to save the resources, the nodes may act as selfish. To avoid the above issues, we place a sensor node called as mobile sink which act as an intermediate between the cluster-head and the base station. The mobile sink (MS) is kept in moving state so that the intruder may not find the location of the node easily. The proposed cluster-based wireless sensor networks topology is shown in the figure 2.The mobile sink gathers the data from each of the cluster-head when it moves near to the corresponding clusters. The mobile sink reduces the work load of the cluster-head. When the cluster-head transmits the data to the mobile sink, the energy of the cluster-head reduces.

B. Cluster- Head Election

The cluster-head is elected for the first time based on energy consumption. Any node in the particular cluster can be elected as a head for the initial stage. In a particular cluster, the sensor nodes would be given a chance to elect their leader. For e.g. in round r, if the 5^{th} node is elected to be a head then for the next round r+1, the 5^{th} node cannot act as cluster head. The cluster-head election in the proposed scheme is based on energy consumption of the sensor nodes. The algorithm proposed in [7] gives the idea of considering three various factors in electing the head. The three factors considered are: a) remaining battery time, b) distance, c) speed. Since the nodes here are fixed, we do not consider the speed. Hence, we focus on the other two factors distance and battery power. The proposed algorithm works in the following manner:

1. For 1^{st} round, a CH is elected based on energy consumption.
2. For the next round, same node cannot act as CH.
3. When MS gathers data from CH, it sends a message to the cluster with regards to change the CH.
4. In this case, the remaining battery power and the distance between the CH and other nodes are calculated.
5. The values calculated are stored as Eligibility Factor which is calculated as
   $EF_i(t) = w_1 B_i(t) + w2D_i(t)$
   Where,
   $B_i(t)$ - Remaining battery power of node i at time t.
   $D_i(t)$- Distance of a node i to the center calculated at time t .
   w1, w2 - Weighting factors that reflect the importance of each parameter and w1+w2 =1.
6. The node with highest value of eligibility factor amongst all nodes involved in the election procedure is elected as CH.
7. The other factor that is considered during the CH is the trust level of the nodes.
8. If the node with highest EF is found to be selfish, then the node would be rejected in being selected as CH.

This algorithm will help in increasing the trust level of nodes and also helps in detecting the best CH easily and efficiently. The cluster-head election is very important because the CH in each cluster gathers the data from all the sensor nodes present in their corresponding clusters. The battery power is one of the main factors that are to be checked very often. If the nodes are out of battery, then a node should be placed in that location.

C. Reduce False Positive Rate

The main advantage of using the signature based detection is low false positive rate. The IDS agents are trained to identify the intruder that enters in the network. The flow of the proposed work is shown below.

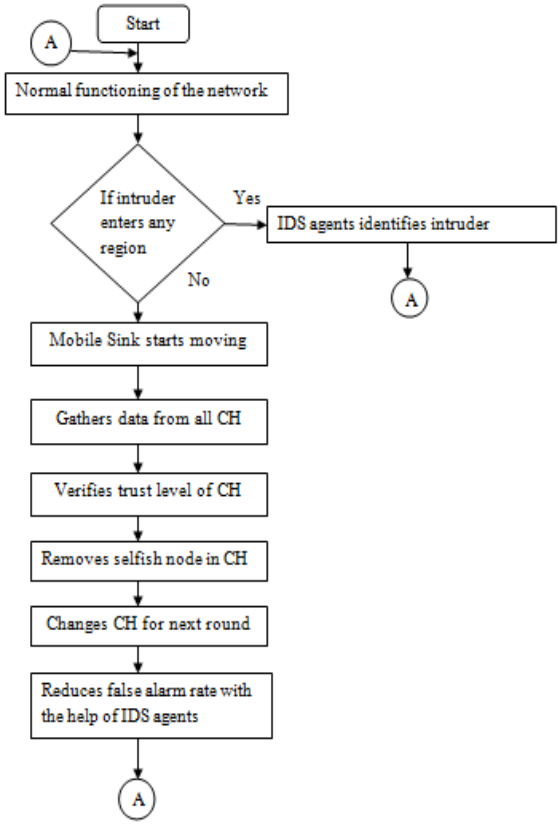

Figure 3: Flow of the proposed work

Here, the IDS agent is equipped with an Audit Data System (ADS) and Intrusion Detection Framework (IDF). The cluster head agent is equipped with Collaborative Detection System (CDS).

1) ADS: IDS nodes gather the packets within their radio range and pass it to the intrusion detection framework.
2) IDF: The intrusion detection uses anomaly and signature detection techniques. The signature detection contains a set of fixed rules to detect the attack and the anomaly detection contains the SVM classification to classify the type of attack.
3) CDS: In the collaborative process, a vote mechanism is applied. CH takes on this mechanism to see if there is any intruder.

The signature detection technique will help in achieving low false positive rate and the anomaly detection helps in identifying the new attacks in the network. The anomaly detection helps in achieving high detection rate. The proposed work will increase the energy level in the nodes.

5. Empirical Evaluation

The mobile sink gathers data from all cluster-head and improves the energy level of the cluster-head. It detects selfish node easily and efficiently, also it decrease the false detection rate up to some extent. The IDS agents are trained well to identify the type of attack. These works makes the network to be secured from various attacks. Also, the IDS agents used in the network help in achieving high detection rate and low false positive rate.

The comparison x-graph between the existing scheme and the proposed scheme is shown in the following figure.

Figure 4: Comparison x-graph

6. Conclusion

The above proposed model is implemented in the clustered topology. The mobile sink is kept moving around the clusters for gathering the periodic updates from each cluster. The trust level of the cluster is verified by the mobile sink in the implementation. The selfish nodes in the cluster will be removed and high level of trust is provided to the network with the concept of dynamic IDS and intrusion detection framework.

References

[1] R. Roman, J. Zhou, and J.Lopez, "Applying Intrusion Detection Systems to Wireless Sensor Networks", the 3rd IEEE Consumer Communications and Networking Conference, 2006, pp.640-644.
[2] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless Sensor Network Security: A Survey", Security in Distributed Grid and Pervasive Computing, Auerbach Publications, CRC Press, Vol.1, Issue.2, 2006, pp.1-50.
[3] Hichem Sedjelmaci, Sidi Mohammed Senouci, Mohammed Feham, "Intrusion Detection Framework of Cluster-based Wireless Sensor Network", IEEE 2012.
[4] K. Q. Yan, S. C. Wang, S. S. Wang, and C. W. Liu, "Hybrid Intrusion Detection System for Enhancing the Security of a Cluster-based Wireless Sensor Network", In Proc. 3rd IEEE International Conference on Computer Science and Information Technology, Chengdu, China, 2010, pp.114-118.
[5] S. M. Hosseinirad and S.K. Basu, "Imperialist Approach to Cluster Head Selection in WSN", In Proc, Special Issue of International Journal of Computer Applications

(0975 – 8887) on Wireless Communication and Mobile Networks, No.1. Jan.2012, ww.ijcaonline.org.

[6] Naveen Kumar Gupta, Ashish Kumar Sharma and Abhishek Gupta, "Selfish Behaviour Prevention and Detection in Mobile Ad-Hoc Network Using Intrusion Prevention System (IPS)", In Proc IJRREST: International Journal of Research Review in Engineering Science and Technology (ISSN 2278- 6643) Volume-1 Issue-2, September 2012.

[7] J. Cynthia, V. Sumathi and S.Arul Jothi, "Adaptive Service Provisioning for Mobile Ad-hoc Networks", In ICTACT JOURNAL on communication technology, September 2010, issue: 03.

[8] Abduvaliyev .A, Lee.S, and Lee .Y .K (2010), "Energy efficient hybrid intrusion detection system for wireless sensor networks", International Conference on Electronics and Information Engineering, IEEE, Kyoto,Japan,2010, pp.25-29.

[9] Huo.G, and Wang.X (2008), "A Dynamic Model of Intrusion Detection System in Wireless Sensor Networks", In Proc. International Conference on Information and Automation, IEEE, Zhangjiajie, China, 2008, pp.374-378.

[10] http://www.isi.edu/nsnam/ns/tutorial/

[11] http://www.cs.berkeley.edu/

[12] www.winlab.rutgers.edu/~zhibinwu/html/ network_simulator_2.html

Author Profile

Madhumathi did her B.Tech IT at Coimbatore Institute of Engineering and Information Technology in 2005-2009. She completed her M.E CSE at United Institute of Technology in2011-2013. She is currently, working as Assistant Professor in the Department of Computer Science and Engineering at KPR Institute of Engineering and Technology.

Guru Siva Kumar did his B.Tech IT at Coimbatore Institute of Engineering and Information Technology in 2005-2009. He completed his M.E CSE in the Anna University Regional Centre, Coimbatore. Currently, he is employed as Career Skill Trainer – PMO at Kumaraguru College of Technology, Coimbatore, India