International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878, Impact Factor (2014): 3.05

Efficient Cluster Head Selection and Mobile Sinks for Cluster-Based Wireless Sensor Networks

Madhumathi C S[1], Guru Siva Kumar T K[2]

[1]Assistant Professor, Department of CSE,
KPR Institute of Engineering and Technology, Coimbatore, India

[2]Career Skill Trainer – PMO,
Kumaraguru College of Technology, Coimbatore, India

Abstract: ***Security for Wireless Sensor Networks (WSN) is an area that is to be considered in order to protect the data they convey and the location of their members. Energy is a scarce resource in the sensor networks and it has to be used efficiently. To reduce the energy consumption of the nodes, we propose the idea of including an additional node called as mobile sink (MS) in Cluster-based WSN (CWSN). The MS acts like an intermediate between the cluster-head (CH) and the base station (BS). The biggest threat to the sensor networks is the attack of the intruder. To prevent the system from intruder, Intrusion Detection System (IDS) agents are trained about the attacks. The existing scheme just checks the sensor nodes present in the cluster for intruder where as the cluster head is not verified for intruder. The existing cluster-head election is done based on the consumption of energy. We propose adaptive leader election scheme that makes use of an eligibility factor that is calculated based on the remaining battery time and the distance. In CWSN, the mobile sink is dynamic that collects the data from all the CH and then transfers it to the BS. The CH for each round changes based on the adaptive leader election and if any intruder enters into the network at any time, the IDS agents identify the intruder. This change in the proposed scheme uses the energy more efficiently and increases the network lifetime thereby decreasing the false positive rates in the network.***

Keywords: Intrusion, Clustering, Intrusion Detection System, Mobile Sink, Adaptive leader election

1. Introduction

Wireless Sensor Networks (WSNs) offer an excellent opportunity to monitor environments and it has a lot of interesting applications in warfare. The problem is that the various security mechanisms used for wired networks do not transfer directly to sensor networks. The reason is that there is no person controlling each of the nodes and even more importantly, energy is a scarce resource. These applications are required often to be deployed in hostile environments, where nodes are attractive target to attackers. Wireless networks have gathered great growth which has given rise to new research challenges. Many researchers have so far focus on the individual aspects of security that are capable of providing protection against specific types of attacks. Recent years, many cryptographic-based security solutions have been proposed. Even though there are many security solutions, only less importance is given to intrusion detection issues of WSNs. The proposed cryptographic solutions alone cannot prevent all possible attacks.

Security is becoming a major concern for protocol designers of WSN because of the broad security-critical applications of wireless sensor networks (WSNs). To protect a network, there are usually several security requirements such as availability, freshness, quality of service, confidentiality, integrity, and authenticity which should be considered in the design of a security protocol. An effective security protocol should provide services to meet these requirements. In many cases, no matter how carefully we design a security infrastructure for a network, attackers may still find a way to break into it and launch attacks from the inside of the network by acting as one of the original node. If they just keep quiet in the network by just listening to the data there is a chance for those nodes without being detected. If they behave more actively to disrupt the network communications then it will be denoted as anomalies which will be indicated as the existence of malicious intrusion or attacks.

2. Intrusion Detection System

An Intrusion Detection System (IDS) detects a security violation on a system by monitoring and analyzing network activities, and sounds an alarm when an intrusion occurs. There are two kinds of approaches: misuse detection (signature-based) and anomaly detection. Misuse detection helps to identify the unauthorized user from signatures while anomaly detection identifies from analysis of an event. When either of the two techniques detects violation, it will raise an alarm to warn the system which will responds to it. The IDS is used to protect the network against both internal and external attacks. The task of this method is to analyze a target node and trigger an alarm when suspicious activities occur.

We believe that IDS is useful and more effective to detect any malicious behavior that attempts to launch either internal or external attacks. In [1] Roman claims that IDS solutions for ad-hoc networks cannot be applied directly to wireless sensor networks. This is assumed to be true as sensor networks introduce severe resource constraints in data storage and power consumption [2].

In the literature, intrusions detections are classified into two categories as shown in “Figure 1”.

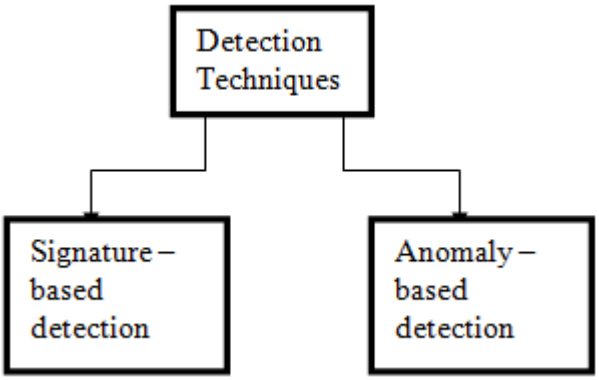

Figure 1: Detection techniques

Signature-based detection: the action or behavior of nodes is compared with well-known attack patterns. In this case, attack patterns must be defined and given to the system. The disadvantage of this technique is that it needs the knowledge to build attack patterns. These systems are not able to detect novel attacks and there is need for someone to update the attack signatures in the database often.

Anomaly-based detection: this technique compares behavior of observed nodes with normal behaviors rather than attack patterns. This model first describes normal behaviors which are established by automated training and then flags the intrusions from the activities varying from these behaviors. The disadvantages of this system can exhibit legitimate but unseen behavior which leads to a substantial false alarm rate. Also, an intrusion that does not contain any symptom of anomalous behavior may not be detected, which results in false negatives.

A new IDS model that combines the advantage of anomaly and signature based detections (high detection rate and low false positive respectively) in order to obtain an efficient detection system to identify malicious nodes is used as referred in [3].

The outline of this paper is organized as follows: In Section 3, we highlight some of the related work that was carried out so far in the existing literature. The proposed scheme is presented in Section 4. Finally we conclude this paper by showing the comparison graph on how the energy is used more efficiently than the existing scheme.

3. Related Work

Previous literatures focus on the hybrid intrusion detection model which combines both the anomaly detection and the misuse detection. The cluster head election is also done based on energy consumption and other various algorithms.

The authors in [1] deal with the Intrusion Detection Systems (IDS) which is a mature area in wired networks, which has attracted many attentions in wireless ad hoc networks recently. The task of Intrusion Detection Systems (IDS) is to monitor computer networks and systems, to detect the possible intrusions in the network, and to alert the users after intrusions had been detected and to reconfigure the network if possible.

In enhancement to the previous approach the authors in [3] Hichem, Sidi &Feham proposed a new IDS model that combines the advantage of both misuse based and anomaly based detection. The anomaly detection uses a distributed training algorithm for the SVM to distinguish between the normal and the anomalous activities. A set of fixed rules related to each attack signature are stored at each node. The concept of clustering topology is used that divides the sensor network into a set of clusters, each one having a CH. Each node has the possibility to activate its IDS. The IDS agent is equipped with an Audit Data System (ADS) and Intrusion Detection Framework (IDF). The cluster head is equipped with Collaborative Detection System (CDS).

The authors K.Q.Yan, S.C.Wang & C.W.Liu [4] proposed an Intrusion Detection System (IDS) for CWSN. The capability of Cluster Head (CH) is better than other Sensor Nodes (SNs). Therefore, a Hybrid Intrusion Detection System (HIDS) is designed and the CH is used to detect intruders that decreases the consumption of energy and also efficiently reduces the amount of information in the entire network. HIDS consists of three models: the anomaly detection model, misuse detection model and decision making model. The anomaly and misuse detection model is used to detect intrusion and to filter a large number of packet records. The decision making model determines the intrusion and classifies the type of attack.

The authors in [8] used specification- based detection in addition to the anomaly and misuse detection. The process takes place in the following way. First, the packets delivered to anomaly detection model are checked for abnormal activities. If model finds that intrusion is not occurred, the packets will be successfully forwarded to the base station. Suppose if anomaly detection model finds that intrusion is occurred, then the packets is forwarded to misuse detection model and decision making model. The model compares received information with predefined patterns of normal attacks, and then the model sends the results to decision making model. The information derived from both techniques is used as an input for decision making model. It integrates the outputs of anomaly and misuse detection models in order to decide whether intrusion is occurred or not. In case of presence of an intrusion, the model reports the results to the administrator of the network.

In contrast to the above approaches, the author [9] proposed dynamic IDS for WSN which has a remarkable improvement in the area of security, stability and robustness issues as compared to static IDS. The process takes place in the following way: the sensor nodes are first deployed. Then IDS is activated in certain nodes in clusters to detect intruders. Then if one of the IDS nodes has consumed 30 percent of the overall energy which it has before activating its IDS, clusters reconfigure and IDS will be activated in new nodes and in new clusters. Then the algorithm goes to iteration. Due to different energy overheads in nodes, new cluster will differ from the original one according to clustering reconfiguration algorithm every time.

For example, cluster heads will change every time after reconfiguration. So the clusters are changing at intervals and IDS are moving as well, which forms a dynamic model. Then,

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.

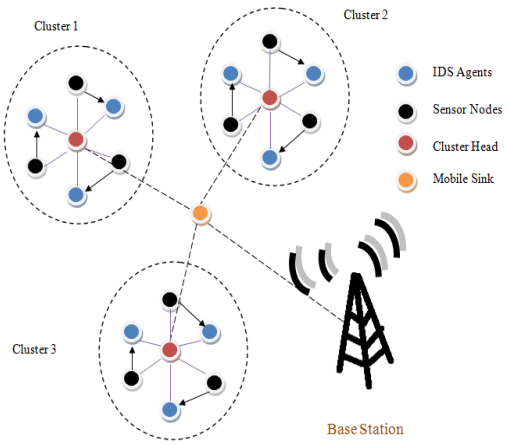

Figure 2: Proposed CWSN topology

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.

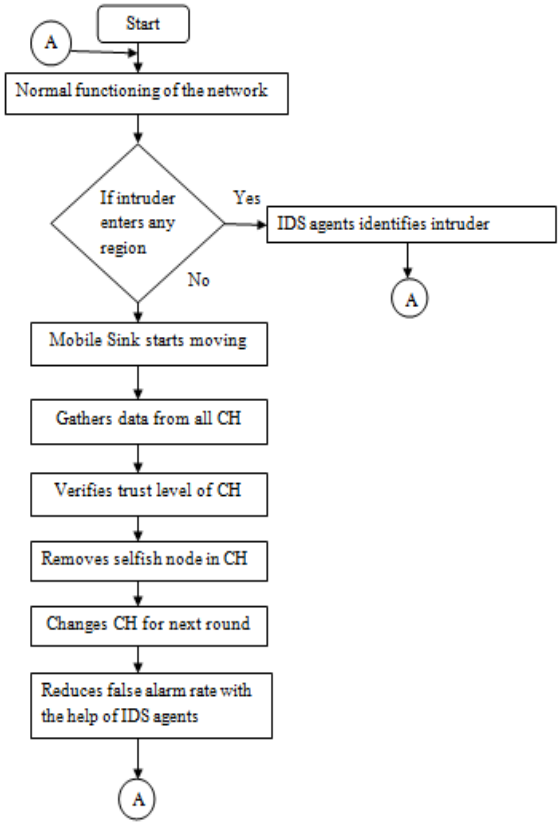

Figure 3: Flow of the proposed work

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