International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 3, Issue 6, June 2016

Advanced Intrusion Detection System for Wireless Sensor Networks

[1]Rummana Firdaus [2]Ambika V
[1][2]Assistant professor,
[1][2]Department of Computer Science & Engineering,
GSSS Institute Of Engineering And Technology For Women, Mysuru
[1]rummana@gsss.edu.in, [2]ambikav@gsss.edu.in

***Abstract* - Wireless Sensor Network consists of large number of nodes which are deployed over a geographical area. Security is a very important consideration while designing a Wireless Sensor Network. So an Advanced Intrusion detection System has been proposed where the Hybrid Intrusion Detection System(HIDS), Energy Prediction based Intrusion Detection System (EPIDS) as well as the Cross layer Detection System are implemented In various stages in order to assure maximum possible security from the Intrusions. Energy Prediction Approach alone is not suitable for the WSN, so HIDS which is suitable for large and sustainable WSN's is combined. Also combining these two approaches along with the Cross Layer IDS make it suitable for a large WSN also. So the new proposed IDS will offer a wide range of flexibility for its application in any type of Wireless Sensor Networks.**

Keywords: Wireless Sensor Network, Intrusion Detection System, HIDS, Cross layer, Nodes, Energy Efficiency

I. INTRODUCTION

Wireless sensor network is a new technology which is becoming more popular and useful in many areas like military application, environmental monitoring, home application, health or medical application, industrial monitoring, structural strength monitoring etc.[1]. Over the years, it has emerged as a competent technology. The major function of wireless sensor networks (WSN) is to collect and monitor the related information which about the specific environment. The sensor nodes (SN) detect the surrounding environment or the given target and deliver the data to the sink using wireless communication. The data is then analyzed to understand the state of the target. However, due to the design of their hardware, WSNS suffer from many resource constraints, such as low computation capability, small memory and limited energy[2]. 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 differs in their characteristics like separation of distance, energy level etc based on the application area. Also wsns are vulnerable to many types of security attacks. Self-organizing nature, low battery power supply, transmission medium's broadcast nature, limited bandwidth support, distributed operations using open wireless medium, multihop traffic forwarding, and dependency on other nodes are such characteristics of sensor networks that expose it to many security attacks at all layers of the OSI model. Security attacks against WSNs can be classified as active and passive. Passive attacks are silent in nature and are conducted to extract important information from the network. Passive attacks do not harm the network or network resources. Active attacks are used to misdirect, temper, or drop packets.

Many security solutions for WSNs have been proposed, 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. 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 two or more IDSs are found to be effficient. So in order to achieve a perfect defence from the intrusions, a three layered component is proposed which consist of monitoring component, analysis and detection component and alarm component.

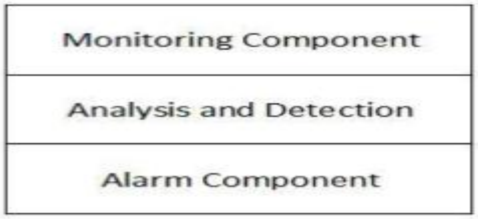

Fig- 1

Broadly speaking, IDS has three main components [3] as shown in Figure 1.(i)Monitoring component is used for local events monitoring as well as neighbours monitoring.

This component mostly monitors traffic patterns, internal events, and resource utilization [24].(ii)Analysis and detection module is the main component which is based on modeling algorithm. Network operations, behavior, and activities are analyzed, and decisions are made to declare them as malicious or not.(iii)Alarm component is a response generating component, which generates an alarm in case of detection of an intrusion.

II. RELATED WORK

A. Signature and Anomaly based Intrusion Detection Systems

There are 2 basic classes of IDSs called as signature based IDSs and anomaly based IDS [5]. In signature based IDS, the signature or properties of different security attacks are maintained in the database. The IDS is very effective in the case of well-known security attacks but when new security attacks arises, the detection rate is very low because the signatures are not included in the database. In the case of anomaly based IDS, it detects the new IDS but misses the well-known attacks.

B. Hybrid Intrusion Detection System

A Hybrid intrusion Detection System (HIDS) [2] is a combination of Signature based as well as the anomaly –based IDSs. It not only has the advantages of both the IDSs. It has their limitations too. Both well-known, as well as new intrusions or attacks can be detected using this. So it works well compared to the Signature based or the Anomaly- based IDSs [6] used separately. But the disadvantage is that only a few type of intrusions will be detected. When it comes to a large network where the intrusions are internal as well as external, HIDS seems to be less beneficial.

C. Energy Prediction based Intrusion Detection System

The battery power is an important factor which plays an important role and determines the lifetime of the network. So keeping in view the power limitation of the WSN's, it is desirable to design power efficient mechanism for sustainable WSNs. The attacker will not allow the sensor nodes to switch to sleep mode in energy exhaustion attack. In sleep mode the sensor nodes will consume less energy.

In energy exhaustion attack, unnecessary data will be sent intermittently the sensor nodes and keeps it always busy [7]. Also as it is deployed in hostile Environment, many physical attacks such as battery replacement node destruction, replacement of nodes, replication of nodes and node reprogramming with a malicious node will be affected. So the Energy Prediction based Intrusion Detection System (EPIDS) will calculate the initial energy of the nodes and the consumption rate for the normal functioning of the nodes will be preprogrammed. Any Consumption rate other than this will be indicated by the IDS.

D. Cross Layer Intrusion Detection System

Traditional IDS operates at a single layer of the OSI model and hence can monitor and detect intrusions at that particular layer. For example, network layer Intrusion Detection System can detect only routing attacks but cannot respond to MAC, physical, or transport layer anomalies. Cross layer IDSs have the capability to monitor and detect intrusions at multiple layers by communicating and exchanging parameters amongst different layers using cross layer interface. A WSN will be divided in to different clusters [6] having a cluster head and other cluster members. The different steps which are implemented in this IDS are, firstly a list of suspected nodes will be found out by estimating the attacked area. Inconsistency in the data can be found by the base station by using the statistical method described as follows.
Let X1…………..Xn be the sensing data collected. Let X be the mean. Then,

$$F(Xj)= \sqrt{((Xj- X)2/x)}$$

If Xj is greater than a threshold value, a node became suspicious, because the date from this particular node will be different from other nodes. In the second phase of the Cross layer IDS, the intrusion will be identified by analyzing the routing pattern in the area which is affected.

III. PROPOSED METHOD

In this IDS, the combination of Energy Prediction based IDS, Hybrid Intrusion Detection System as well as the Cross Layer IDS will be implemented.

A. Cluster Head Selection

As the WSN consists of different nodes, the cluster head selection is an important procedure in this IDS, The algorithm is as follows:[7]

```
Si – Set of type i sensors in the WSN area.
S- Set of all sensors in the network.
N(a)- Set of neighbours of node a.
Repeat
For i=1 to N
Select node a with min N(a) in Set Si
            If N(a)≠ ϕ
             Select a
SN= j/the distance between a and N(a)< (rsi/2)
 If SN>1
 S=S-(SN U a)
Else
 S=S-a
Until S is null set
```

In this way the cluster head will be formed. The cluster head will be having the maximum amount of energy as compared to the other sensor nodes.

E. A packet is determined to be abnormal by the system when the current behaviour varies from the model of normal behaviour.
Step 1: Analyzing the packet's historical records of Cluster based WSN.
Step 2: Feature selection. To find the features, which have identifiable properties, compare the normal and abnormal packets to find the features, which determine normalcy to develop rules
Step 3: Establishing the rules in anomaly detection model.

F. The decision making model is used to combine the outputs of the anomaly detection and misuse detection models. It determines whether or not an output is an intrusion, and the category of attack. It then has to report the results to the administrator to help them handle the state of the system and make further corrections.

IV. CONCLUSION

We know that security is the main criteria while designing a Wireless Sensor Network. Due to the Broadcast nature of the medium, they are more prone to security attacks. In this paper, an Advanced Intrusion Detection System has been proposed. It improves the detection rate and efficiency so that almost all the Intrusions can be detected. Also the system is applicable to small, medium as well as large sized networks. That means it gives a wide range of flexibility in detection of Intrusions compared to the other existing systems. Also the energy efficiency and the system life time is greatly improved. Other methods to select features can be used in the future, such as data mining, to find identifiable features, instead of relying on the viewpoint of experts.

REFERENCES

[1]. Sivaprakash S et.al "Cluster Based Intrusion Detection System for Wireless Sensor Networks", International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

[2]. K.Q. Yan et.al "A Hybrid Intrusion Detection System of Cluster-based Wireless Sensor Networks", Proceedings of the International MultiConference of Engineers and Computer Scientists 2009 Vol I IMECS 2009, March 18 - 20, 2009, Hong Kong

[3]. Ms. Rachana Deshmukh et.al "An Intrusion Detection Using Hybrid Technique in Cluster Based Wireless Sensor Network", Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 4, Jul-Aug 2013

[4]. Kanojia Sindhuben Babulal et,al "Cross Layer Design for Cooperative Transmission in Wireless Sensor Networks", Wireless Sensor Network, 2011, 3, 209-214 doi:10.4236/wsn.2011.36024 Published Online June 2011 (http://www.SciRP.org/journal/wsn)

[5]. Abror Abduvaliyev et.al "On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks", IEEE Communications Surveys & Tutorials, Vol. 15, No. 3, Third Quarter 2013

[6]. Fatma Bouabdallah et.al "Cross-Layer Design for Energy Conservation in Wireless Sensor Networks", INRIA, Campus universitaire de Beaulieu ; 35042 Rennes Cedex, France

[7]. Fereshteh Amini "Intrusion Detection in Wireless Sensor Networks", Security in Distributed, Grid, and Pervasive Computing Yang Xiao,(Eds.) pp-- 2006 Auerbach Publications, CRC Press