A Survey on Intelligent Intrusion Detection System in Wireless Sensor Networks

S.Yamunarani, D.Sathya

Abstract- **The Wireless Sensor Networks (WSNs) are highly distributed networks of tiny, light-weight wireless nodes, placed in large numbers to monitor the environment or system. Monitoring the system includes the measurement of physical parameters such as temperature, pressure, relative humidity and co-operatively passing their data to the main location (sink). Intrusion Detection is one of the major and efficient method against attacks. Intrusion Detection Systems can act as a second line of defence and it provides security primitives to prevent attacks against computer networks. IDS uses misuse-based and anomaly-based detection techniques. This paper discuss different approaches of IDS.**

***Index Terms*—Wireless sensor networks, Intrusion Detection System, sensor nodes.**

I. INTRODUCTION

The Wireless Sensor Networks consists of sensor nodes ranging from few hundred or even thousands depending on the application. Each sensor node may be connected to one or more other sensor nodes. Each node of the sensor network consists of four components namely, sensing unit, processing unit, transceiver unit and the power unit.In addition to the above units, a wireless sensor node may include a number of application-specific components. For this reason, many commercial sensor node products include expansion slots and support serial wired communication.

Wireless sensor nodes typically do not have very much computational power, it limits the kind of networking protocols and security techniques it can use. Batteries have a short lifetime and cannot be replaced on sensor nodes since they are usually deployed in a hostile environment. Due to the low computational capabilities and energy resources of sensor nodes security mechanisms used for wired networks do not transfer directly to wireless sensor networks.

WSNs consist of many low-cost, tiny devices, and usually arranged to an open and insecure region, they are susceptible to various types of attacks. For example, when WSN is placed to the battlefield, SNs are invaded by the enemy and destroyed. Thus, the security of the WSN needs to be measured. A prevention method is used to counteract familiar attacks. It establishes a corresponding prevention method, according to the characteristics of an attack. However, prevention mechanisms cannot resist overall attacks. Therefore, it is necessary to detect the attacks, using an Intrusion Detection System (IDS). IDS is used to detect the packets in a network, and determine whether they are attacker nodes. in addition, IDS can help to develop the prevention method through acquired natures of attack.

Detection based techniques aim at identifying the intrusions that affect the network infrastructure after a failure of the prevention based techniques. In our work we focused on intrusion detection systems applied to wireless sensor networks. The two major models of intrusion detection include anomaly detection and misuse detection .Anomaly detection builds a model of normal behaviour and compares the model with detected behaviour. Anomaly detection has a high detection rate, but the false positive rate is also high. The misuse detection model is built, so that the attack type is determined by comparison with the attack behaviour. The misuse detection has high accuracy, but the detection rate is lower. The misuse detection cannot detect unknown attacks in the networks.

II.INTRUSION DETECTION SYSTEMS IN WSN

The threats that damage the security of WSN can be detected by using IDS. The IDS attempts to identify computer system and network intrusions and misuses by gathering and analyzing data. The purpose of IDS is to serve as an alarm for computer system and network. The information which contains unwanted and misbehaving elements. It isolates the misbehaving elements to deny them from network and computer system.There are three main approaches that an IDS can use to classify the attacks:

A) Misuse detection:

It is also called as Signature based IDS. It is used to find attack type by comparing it with attack behavior. The signature of known attacks are stored and when the attacks matched with the signature then it finds or signals as an intrusion. It has high accuracy. The disadvantages of the system has detection rate is lower and it finds only known attacks of the system, if any unknown attacks occurs, it does not detect it whose signature are not known.

B) Anomaly detection:

This technique is used to build model of normal behavior and compare it with detected behavior .It has high detection rate and ability to detect unknown attacks as well as "Zero day" attacks and anomaly modeled with normal operation ,so it can detect unknown attacks when normal operations deviates from them. Normal activities are customized for every system, application and network so it is difficult for an attacker to know what activities it can carry out without getting affected. The disadvantage has false positive rate.

C) Specification-based detection:

This technique combines the aims of misuse and anomaly detection mechanisms, as it is focused on discovering deviations from normal behaviors that are defined neither by machine learning techniques nor by training data. In fact, the specifications that describe what can be considered as normal behavior are defined manually. Any action is monitored with respect to these specifications. The drawback of this approach is the manual development of all specifications, which is a time-consuming process for human beings. Another disadvantage of this technique is that it cannot detect malicious behaviors which do not violate defined specifications of the IDS protocol.

It contains three main modules in intrusion Detection and it is classified as

A)Monitoring Module:

It controls the collection of data.

B)Analysis Module:

It deciding if the collected data contains any intrusions or not.

C)Response Module:

It managing the response actions to the intrusions.

III. MAJOR ISSUES IN WSN

A. Security

Security in a sensor network is very challenging in WSN is not only being deployed in battlefield applications but also for surveillance and building monitoring applications.

B. Quality of service

The QOS in WSN is difficult because the network topology may change constantly.

C. *Localization*

The sensors are placed lacking their position in advance and once it is deployed there is no supporting infrastructure available to locate and manage them.

D. *Deployment*

Sensor nodes can be deployed either by placing one after another in sensor field or by dropping it from the plane. Sensor nodes are placed in real world, node death due to energy exhaustion either caused by normal battery discharge or due to short circuits is a common problem which may lead to wrong sensor readings.

E. *Medium Access Control*

Communication is a major source of energy consumption in WSN and MAC protocol directly control radio of nodes in network.MAC protocol should avoid collisions from interfering nodes.

IV. DESIGN CHALLENGES OF WSN

A. Scalability

The network must preserve its stability. Introducing more nodes into the network means that additional communication messages will be exchanged, so that these nodes are combined into the existing network.

B. Fault tolerance and adaptability

Fault tolerance means to maintain sensor network functionalities without any interruption due to failure of sensor node because in sensor network every node have limited power of energy so the failure of single node doesn't affect the overall task of the sensor network.

C. Node Deployment

Sensor network can be deployed randomly in geographical area. After deployment, they can be maintained automatically without human presence.

D. Power Consumption

Wireless sensor node is microelectronic device means it is equipped with a limited number of power source. Nodes are dependent on battery for their power. Therefore power preservation and power management is an important issue in wireless sensor network.

E. Production Cost

As the name suggests production cost, we know that in the sensor network we have large no of nodes deployed, so if a single node will be very high then the cost of overall network will be very high.

F. Limited Computational Power and Memory Size

It is another factor that affects WSN in the sense that each node stores the data individually and sometime more than one node stored same data and transferred to the base station which wastes the power and storing capacity of nodes so we must develop effective routing schemes and protocols to minimize the redundancy in the network.

G. Security

Security is very important parameter in sensor network since sensor networks are data centric so there is no particular id associated with sensor nodes and attacker can easily inserted himself into the network and stole the important data by becoming the part of network without the knowledge of sensor nodes of the network. So it is hard to identify whether the information is legal or not.

V. LITERATURE SURVEY

A. Applying Data Mining Techniques to Intrusion Detection in Wireless Sensor Networks

In [4], is the second line of defence and it gives security to prevent attacks against computer network. In proposed, hybrid, lightweight, distributed IDS for WSN are discussed. Hybrid composed of central agent perform accurate IDS by using Data mining Techniques. In proposed system a hybrid, lightweight, distributed Intrusion Detection System (IDS) for wireless sensor networks are used. This IDS uses both misuse-based and anomaly-based detection techniques. The compared techniques are Classification And Regression Tree(CART), Chi-squared Automatic Interaction Detection(CHAID), C5.0, Logistic Regression, Bayesian Network . According to the experimental results, the best detection techniques are C5.0 and CART since they are more accurate, and they also show lower false positive rate, that implies low energy consumption for alert communication from Local Agents to the Central Agent.

B. An Integrated Intrusion Detection System for Cluster-based Wireless Sensor Networks

In [7],Sink and cluster head are easily attacked by enemies, so the security is necessary. The capabilities of all sensors in CWSN are heterogeneous. Due to different capabilities and probabilities of attack on them, three separate IDS are designed for Sink, Cluster head and sensor nodes. Intelligent Hybrid IDS is proposed, it has learning ability. Hybrid IDS is proposed in cluster head, it is same as IHIDS but it has no learning ability. HIDS not only decreases the consumption of energy but also efficiently reduces the amount of information. Therefore, the lifetime of CWSN can be prolonged. The goal of cluster head to detect attacks efficiently and avoid resource wasting but it retrain the behaviour of new attacks from IHIDS.

The anomaly detection model is used as the first line of defence in IHIDS. Only few packets are actually attacks. The anomaly detection model acts like a filter. Abnormal packets are delivered to the misuse detection model for further detection. Sensor nodes are used in misuse IDS. A simple and fast detection method is used in sensor node to avoid overwork and save resources for the purpose of safety. The misuse detection module utilizes various models of well known attack behaviour and build a model base according to these behaviours. Because the performance in most techniques of intrusion detection is promised through training data.BPN with the supervised learning method is adopted by this study.BPN learns the corresponding relations between input and output variables, and tunes the corresponding weight.

C. A Hybrid Intrusion Detection System of Cluster based Wireless Sensor Networks

In [9], HIDS consists of an anomaly detection model and a misuse detection model and decision making model. Anomaly model uses Rule based method. It filters a large number of packet records, using the anomaly detection model, and performs a second detection with the misuse detection model, when the packet is determined to intrusion. It efficiently detects intrusion, and avoids the resource waste. Misuse detection uses Back Propagation network.

Finally, it integrates the outputs of the anomaly detection and misuse detection models with a decision making model. This determines the presence of an intrusion, and classifies the type of attack. The output of the decision making model is then reported to an administrator for follow-up work. This method not only decreases the threat of attack in the system, but also helps the user handle and correct the system further with hybrid detection. The advantage of decision making model is simple and fast. The proposed model lowers false positive rate and achieves high detection rate and accuracy.

D. Decentralized Intrusion Detection in Wireless Sensor Networks

In [1],WSNs are susceptible to some types of attacks since they are deployed in open and unprotected environments and are constituted of cheap small devices. Preventive mechanisms can be applied to protect WSNs against some types of attacks. There are some attacks for which there is no known prevention methods, such as wormhole. Moreover, there are no guarantees that the preventive methods will be able to hold the intruders. It is necessary to use some mechanism of intrusion detection.

Besides preventing the intruder from causing damages to the network, the intrusion detection system (IDS) can acquire information related to the attack techniques, helping in the development of prevention systems. Detection is decentralized since the IDSs are distributed on network, installed in common nodes. The collected information and its treatment is performed in a distributed way. Distributed Systems are more scalable and robust since it have different views of the network.

E. Cross Layer Intrusion Detection System For Wireless Sensor Network

In [2], we proposed new intrusion detection system based on cross layer Interaction between network, Mac and Physical layer. But all these systems operate in a single layer of the OSI model, or do not consider the interaction and collaboration between these layers. A new intrusion detection system based on cross layer interaction between the network, Mac and physical layers are used. Mac layer uses the cross layer information from network and physical layer in order to detect possible intrusions. Once intrusion is detected various actions such as dropping, flagging neighbour can be taken. In this system using the NS simulator to demonstrate its effectiveness in detecting different types of attacks at multiple layers of the OSI model.

To provide single cross layer IDS to several layers of OSI model instead of offering IDS for each layer. Simulation results demonstrate the performance provided by IDS in terms of prevention and detection of different intrusion types. we used hierarchical cluster based network topology. This topology divides network into several clusters and selects a cluster head node which has greatest energy reserves in cluster.

F. A Rule Based Approach for Attribute Selection and Intrusion Detection in Wireless Sensor Networks

In [10],in this paper new rule based attribute selection algorithm used for detecting intruders in WSN and also different types of attacks in WSN. In different types of attacks we have mainly focussed on DOS attacks by using rule based Enhanced Multiclass SVM algorithm.DOS attacks are more serious than other attacks with respect to energy consumption. The advantage is to reduce power consumption in WSN by reducing number of packets transmitted. The Results show that the proposed algorithm achieved high detection accuracy and reduced false alarm rate with respect to DOS attacks in WSN.

Table 1
Intelligent IDS system detection Results

Detection module	Total # of instance	Total # of attacks	Detected (detection rate)	Missed (missed rate)	False positive (FP rate)
Anomaly	199600	128450	127100 (98.90%)	1300 (1.02%)	710 (1.00%)
Misuse	199600	128450	127900 (99.50%)	500 (0.30%)	125 (0.15%)
Hybrid	199600	128450	128300 (99.80%)	120 (0.1%)	780 (1.15%)

VI. CONCLUSION

Thus the different intrusion detection system and their techniques are studied in this paper. Different techniques are used to improve detection rate and reduce false positive rate and achieves accuracy. In future by applying intelligent techniques such as support vector machines, genetic algorithms, ant colony optimization and fuzzy sets to improve accuracy further and reduce false positive rate and produce accurate results.

VI. REFERENCES

[1] Ana Paula R. da Silva,Marcelo H.T. Martins,Bruno P.S. Rocha,Antonio A.F. Loureiro,Linnyer B. Ruiz,Hao Chi Wong,“Decentralized Intrusion Detection in Wireless Sensor Networks’’, Q2SWinet’05 Montreal, Quebec, Canada, , October 13, 2005.

[2] Djallel Eddine Boubiche1 and Azeddine Bilami, “Cross Layer Intrusion Detection System For Wireless Sensor Network”, International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012.

[3] Kaliyamurthie K. P. and Dr. R. M. Suresh, “Artificial Intelligence Technique Applied to Intrusion Detection”, International Journal of Computer Science and Telecommunications Volume 3, Issue 4, April 2012.

[4] Luigi Coppolino ,Salvatore D’Antonio, Alessia Garofalo, Luigi Romano“Applying Data Mining Techniques to Intrusion Detection in Wireless Sensor Networks’’ Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, 2013.

[5] Manasi Gyanchandani, J.L.Rana, R.N.Yadav, “Taxonomy of Anomaly Based Intrusion Detection System: A Review “, International Journal of Scientific and Research Publications, Volume 2, Issue 12, 1 ISSN 2250-3153, December 2012.

[6] Prabhakaran Kasinathan, Claudio Pastrone, Maurizio A. Spirito, Mark Vinkovits, “Denial-of-Service detection in 6LoWPAN based Internet of Things”, IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2013.

[7] Shun-Sheng Wang, Kuo-Qin Yan , Shu-Ching Wang , Chia-Wei Liu, “An Integrated Intrusion Detection System for Cluster-based Wireless Sensor Networks’’, Expert Systems with Applications 38 15234– 15243, 2011.

[8] Vokorokos L., A.Balaz and J.Trelova, “ Distributed Intrusion Detection System Self Organizing Map”, INES 2012-IEEE 16th International Conference on Intelligent Engineering Systems, Lisbon, Portugal- June 13–15, 2012.

[9] Yan K.Q., S.C. Wang, C.W. Liu, “A Hybrid Intrusion Detection System of Cluster based Wireless Sensor Networks”, Proceedings of the International Multi Conference of Engineers and Computer Scientists 2009 Vol I IMECS 2009, Hong Kong, March 18 20,2009.

[10] Anand,S.Ganapathy,P.Yogesh,A.Kannan,”A Rule Based Approach for Attribute Selection and Intrusion Detection in Wireless Sensor Networks”,Procedia Engineering 38 1658—1664,2012.