INTELLIGENT INTRUSION DETECTION SYSTEM IN WIRELESS SENSOR NETWORKS

S.Yamunarani[1], D.Sathya[2], S.Pradeepa[3]

[1]Department of Computer Science and Engineering, Kumaraguru College of Technology, Coimbatore, TamilNadu, (India)

[2]Assistant Professor, Department of Computer Science and Engineering, Kumaraguru College of Technology, Coimbatore, TamilNadu, (India)

[3]Assistant Professor, Department of Information Technology , Adithya Institute of Technology, Coimbatore, TamilNadu, (India)

ABSTRACT

Wireless Sensor Networks are highly distributed networks of tiny, light-weight wireless nodes, deployed in large numbers to monitor the environment. 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. Intrusion Detection System can act as a second line of defense and it provides security primitives to prevent attacks against computer networks. The Intelligent Intrusion Detection System has the capability to do different things without any human intervention. Intrusion Detection System uses Misuse-based and Anomaly-based methods. Intelligent Intrusion Detection System technique such as Back Propagation Network, Bayesian Belief Networks and Support Vector Machines are used for detecting cross layer attacks to reduce the false positive rate and improve detection accuracy.

Keywords: Intelligent Intrusion Detection, Wireless Sensor Networks, Back Propagation Networks, Bayesian Belief Networks, Support Vector Machines.

I. INTRODUCTION

The Wireless Sensor Networks [WSNs] 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 which is shown in Fig 1. 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.

Detection based techniques aim at identifying the intrusions that affect the network infrastructure after a failure of the prevention based techniques. In our work it focused on Intrusion Detection System [IDS] 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 behavior and compares the model with detected behavior. From [5], Anomalydetection has a high detection rate, but the false positive rateis also high.

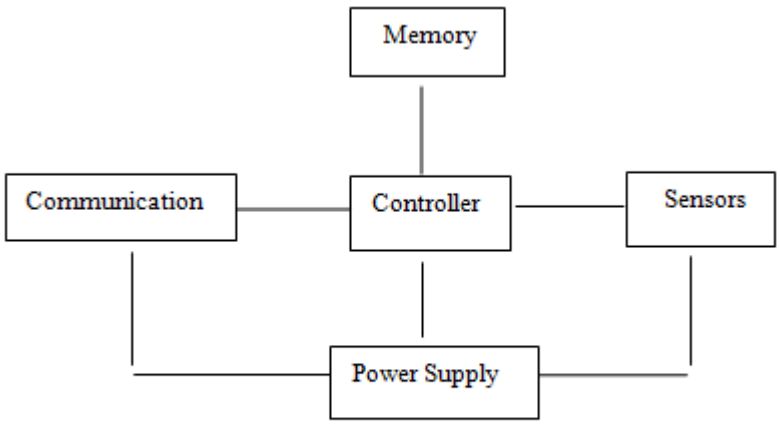

Fig 1. Components of Sensor Node

The advantage of Anomaly detection has the ability to detect unknown attacks by using anomaly IDS. The Disadvantage is, it cannot detect different types of attacks. The Misuse detection model is built, so that theattack type is determined by comparison with the attack behavior. The advantage of Misuse detection has high accuracy, but the detection rate is lower. The Disadvantage of Misuse detection cannot detect unknown attacks in the networks.

The remainder of this paper is organized as follows: InSection 2, works relevant to the common attacks in WSN and the analytic tools of intrusion detection, used in our research, are introduced. In Section 3, the Existing methods are discussed. The simulation results used to evaluate the performance of the existing system are presented in Section 4. The proposed system is discussed. Finally, the conclusion and future work are discussed in Section 5.

II. RELATED WORK

In [4], IDS is the second line of defense and it gives security to prevent attacks against computer network. Hybrid composed of central agent perform accurate IDS by using Data mining techniques. In proposing a hybrid system, lightweight, distributed Intrusion Detection System 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, BayesianNetwork. According to the experimental results, the best detection techniques are C5.0 and CART. The advantages of these two techniques 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.

In [7], sink and cluster head are easily attacked by enemies, so the security is necessary. The capabilities of all sensors in Cluster-Based WSN are heterogeneous. Due to different capabilities and probabilities of attack on them, three separate IDS are designed to sink, Cluster head and sensor nodes. Intelligent Hybrid IDS[IHIDS] is proposed, it has learning ability. Hybrid IDS is proposed by cluster head, it is same as IHIDS but it has no learning ability.

The Anomaly detection model is used as the first line of defense in IHIDS. The anomaly detection model acts like a filter. BPN learns the corresponding relations between input and output variables, and tunes the corresponding weight. The advantage of BPNis a simple and fast detection method is used in the sensor node to avoid overwork and save resources for the purpose of safety.

In [9], HIDS consists of an Anomaly detection model and 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. 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 on 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 a high detection rate and accuracy.

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 wormholes.

Besides preventing the intruder from causing damage 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 a network, installed in common nodes. The collected information and its treatment are performed in a distributed way. The advantage of Distributed Systems is more scalable and robust since it has different views of the network.

In [2], a 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 template protection interaction and collaboration between these layers.A new intrusion detection system based on cross layer interaction between the network, MAC and physical layers is used. MAC layer uses the cross layer information from network and physical layer in order to detect possible intrusions.

To provide single cross layer IDS to several layers of OSI model instead of offering IDS for each layer. Hierarchical cluster based network topology is used in cross layer IDS. This topology divides network into several clusters and selects a cluster head node which has greatest energy reserves in the cluster.

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

III. EXISTING WORK

In [4], Two steps are required for the intrusion detection system setup. They areprofilingand anomaly/misuse detection. The steps of the profiling stage are the following: i) network logs are imported and post-processed; ii)

on the basis of processed messages, decision trees and mean and standard deviation models are produced depending on the Agent that is processing the data. Decision tree approach isused by the Central Agent, that performs a preliminary learning phase by analyzing all network traffic. Local Agents characterize monitoring parameters by estimatingthe mean and standard deviation for the normal behavior; iii) detection rules are defined according to the used technique; iv) the effectiveness of detection rules is tested through experimental data.

3.1 Sinkhole Attack

The purpose of a sinkhole attack is to gain access to alltraffic in the area of the WSN in order to launch moresevere attacks. To reach this purpose, the attacker tries toattract packets to a compromised node that belongs to thenetwork under attack. The sinkhole attack was implemented on the compromised nodes.

3.2 Sleep Deprivation Attack

The purpose of sleep deprivation attack is to hinder nodes from going into sleep mode and saving energy. The consequence is that the low energy resources available on WSN motes are soon consumed and the service offered by attacking nodes is no longer available. The sleep deprivation attack was implemented by flooding the attacked nodes with routing packets, thus forcing the receiver to process the packets and to delay the activation of the sleep mode.

On the compromised node, when routing activities are being performed and the current time is within the attack time window, a packet received is forwarded to target nodes for a high number of times. Even if that packet was discarded by the node (e.g. Because it is a duplicate), the receiver would anyway process the information before discarding it, thus consuming energy resources.

IV. PROPOSED WORK

In the proposed system, it enhanced the work of an existing system by using a decision tree technique and also it deals with Intelligent IDS methods such as Back Propagation Network,Bayesian Classification,Support Vector Machines for detecting cross layer attacks.

In the existing system, IDS acts as a second line of defense to secure the network against the attacks which is not detected by the IPS. In [2], most of the IDS concentrates on the attacks of network layers and leaves the physical, MAC and Application Layer. Most of the work mainly focuses on the stationary data.

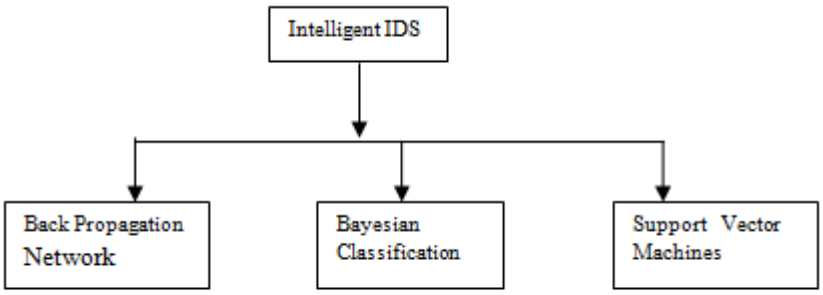

Fig 2: Types of Intelligent IDS

4.1 Decision Tree Method

In [4], Anomaly detection uses threshold metrics in local agent also called as sensor nodes and it sends alerts to the central agent if it finds any abnormalities. Misuse detection uses a decision tree method for central agent also called as a base station for detecting type of attacks. In existing [4],it concentrates only sinkhole attack and sleep deprivation attack. A Decision Tree is a flowchart like tree structure, where each internal node called as non-leaf node denotes a test on an attribute, each branch represents an outcome of the test and each leaf node called as a terminal node contains the class label. The topmost node in a tree called as root node.

4.1.1 Algorithm

Input: Dataset contains the list of attributes and split attributes by using splitting criteria

Output: A Decision tree

Method:

1:create a node K;

2:if the attributes in S are all same class, D then

3: return K as a leaf node labeled with class D;

4:ifattribute_list is empty then

5: return K as a leaf node labeled with majority class in S;

6:applyAttribute_selection_method (S,attribute_list)to findbestsplitting_criteria;

7:Label node K with splitting criteria;

8:if splitting criteria arediscrete_valuedand multiway splits allowed then

9:attribute-list<-attribute-list-splitting attribute;

10:for each result j of splitting-criteria

11:letS_j be set of data attributes in S satisfying results j;

12:ifS_j is empty then

13: attach a leaf considered with majority class in S to node K;

14:elseattach node returned by Generic_decision_tree(S_j,attribute_list) to node K;

endfor

15:return K;

Table 1

Implementation of Decision Tree using Matlab

Technique	FPR	FNR	ACC	TPR	TNR
Decision tree	**0.42**	**0.03**	**0.8**	**0.14**	**0.12**

In[4], network simulator is used for detecting attacks by using Decision Tree. In proposing System, Matlab tool is used for detecting attacks and compare the accuracy values.

Table 2

Accuracy Comparison

Attacks	Accuracy

Sinkhole	**0.7**
Sleep deprivation	**0.8**

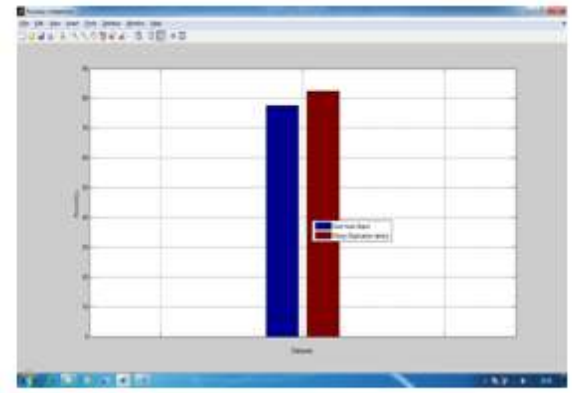

Fig 3: Accuracy comparison between sinkhole and sleep deprivation attack

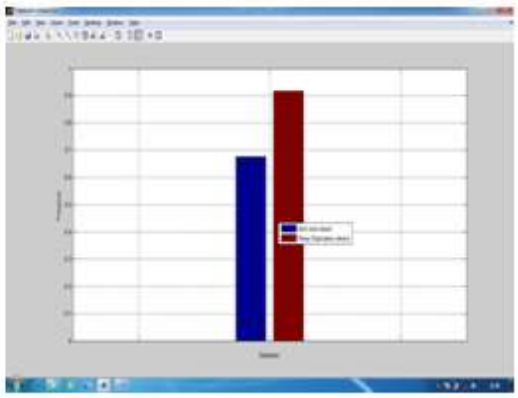

Fig 4: F-Measure Comparison

The complexity in creating large decision trees mandates people involved in preparing decision trees having advanced knowledge in quantitative and statistical analysis. This raises the chance of having to train people to complete a difficult decision tree analysis.

With reference to an existing system [4], the decision tree method is enhanced to improve accuracy better than the existing system and alsoit reduced false positive rates.

4.2 Backpropagation Network

Back Propagation is a neural network learning algorithm. A neural network is a set of connected input/output units in which each connection has a weight associated with it. Neural Network learning is also called as connectionist learning due to the connection between units. The network structure of BPN consists of three layers, as well as an input layer, a hidden layer, an output layer and many links between each layer and each layer has several processing units. The input layer is used to input the outer environmental messages, and by the intersect computing in the hidden layer, a related output is gotten from output layer.

The Back Propagation algorithm performs learning in a multilayer feed forward neural network The units in input layer called as input units. The units in the hidden layer and output layers called as output units.

Input Layer Hidden Layer Output Layer

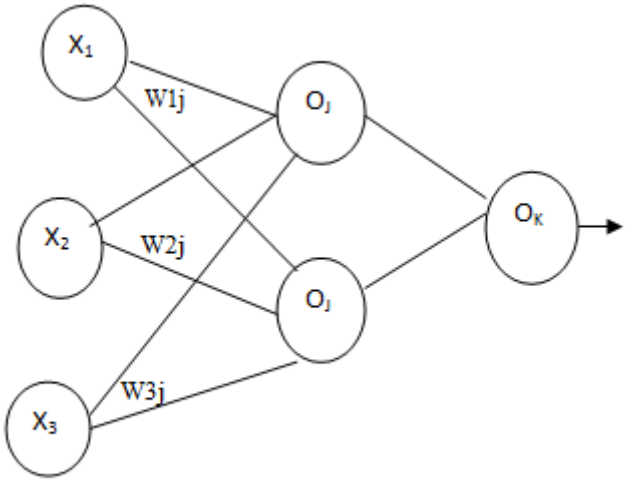

Fig 5: Back Propagation Network

The parameters such as Node id, Path, Source, Destination, Received Signal Strength can be given as input to the input layer and weight values can be combinedand send to the hidden layer. Thenit feed forwards to the output layer. It can verify whether it is normal or abnormal data and it gives results.

4.3 Bayesian Classification

Bayesian classifiers called as statistical classifiers. It can predict class membership probabilities, such as the probability that a tuple belongs to a particular class. It is based on Bayes theorem. It compares with classification algorithm and found simple Bayesian classifier called as a naïve Bayesian classifier. It compares their performance with decision tree and selected neural network classifiers. It has high accuracy and speed when it applies to large databases. The advantage of Bayesian classifiers,it has minimum error rate when compared with other classifiers.

Bayesian belief networks also called as belief networks or Bayesian networks and probabilistic networks. It can also used for classification. It contains two components such as a directed cyclic graph and set of conditional probability tables.

4.4 Support Vector Machines [SVMS]

It is a new method for classification of both linear and non- linear data. It is one of the supervised learning model with associated learning algorithms and it can analyze the data and recognize patterns and used for classification and regression analysis. It constructs hyper plane or set of hyper planes with high dimensional space used for classification, regression and other tasks.

In linear SVM, the classifier is a separating hyper-plane.In non-linear SVM, it locates a separating hyper-plane in the feature space and it classifies points in that space.The kernel function plays the role of the dot product in the feature space. The properties of SVM are Flexibility in choosing a similarity function., It has the ability to handle large feature spaces. SVM has been used effectively in many real-world problems such as text (and hypertext) categorization, Image classification, Bioinformatics(Protein classification, Cancer classification)Hand-written character recognition.

By comparing all these classification techniques and find the best techniques by using these BPN, Bayesian and support vector machine algorithms and find Cross Layer attacks in WSN to improve detection rate and accuracy.

V. CONCLUSION

In the paper, the real sensor mote data are used. The Decision tree approach is implemented for anomaly and misuse detection to improve detection rates and accuracy and reduce false positive rate. It is used to detect sink holes and sleep Deprivation attacks. With reference to an existing system, these two attacks are detected and accuracy is achieved.

REFERENCES

[1] Ana Paula R. da Silva,Marcelo H.T. Martins,Bruno P.S. Rocha, Antonio A.F. Loureiro, Linnyer B. Ruiz,HaoChiWong,"Decentralized Intrusion Detection inWireless Sensor Networks'',Q2SWinet'05 Montreal, Quebec, Canada, October 13, 2005.

[2] DjallelEddine Boubiche1 and AzeddineBilami, "Cross Layer Intrusion DetectionSystem, ForWireless 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 ofComputer Science and Telecommunications Volume 3, Issue 4, April 2012.

[4] Luigi Coppolino,Salvatore D'Antonio, AlessiaGarofalo, 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] ManasiGyanchandani, J.L.Rana, R.N.Yadav, "Taxonomy of Anomaly Based Intrusion Detection System: A Review",InternationalJournal of Scientific and Research Publications, Volume 2, Issue 12, 1 ISSN 2250-3153,December2012.

[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 Ya,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. BalazandJ. Truelove, " 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.

[11] Mohammad SazzadulHoque, Md. Abdul Mukit and Md. Abu NaserBikas, "An Implementation Of Intrusion Detection System Using Genetic Algorithm",International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012.

[12] Dewan Md. Farid1, Nouria Harbi1, and Mohammad ZahidurRahman, "Combining Naive Bayes And Decision Tree For Adaptive Intrusion Detection",International Journal of Network Security & Its Applications (IJNSA), Volume 2, Number 2, April 2010.

[13] K.V.R. Swamy, K.S. Vijaya Lakshmi, "Network Intrusion Detection Using Improved Decision Tree Algorithm",K.V.R.Swamy et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (5), 2012,4971 – 4975.

[14] ManoranjanPradhan, Sateesh Kumar Pradhan, Sudhir Kumar Sahu, "Anomaly Detection Using Artificial Neural Network",International Journal of Engineering Sciences & Emerging Technologies, April 2012. ISSN: 2231 – 6604 Volume 2, Issue 1, pp: 29-36.

[15] Hari Om &TanmoyHazra, "Statistical Techniques In Anomaly Intrusion Detection System",International Journal of Advances in Engineering & Technology, Nov. 2012. ISSN: 2231-1963.