
K.Q. Yan, S.C. Wang* (Corresponding author), S.S. Wang and C.W. Liu
Chaoyang University of Technology
Taiwan, R.O.C.
kqyan@cyut.edu.tw
scwang@cyut.edu.tw

Abstract—Recent advances in Wireless Sensor Networks (WSNs) make them more important to apply. Therefore, security issues are more significant in WSNs. WSNs are susceptible to some types of attacks since they are consisted of cheap and small devices and are deployed in open and unprotected environments. In this research, an Intrusion Detection System (IDS) created in cluster head is proposed. The proposed IDS is a Hybrid Intrusion Detection System (HIDS). It consists of anomaly and misuse detection module. The goal is to raise the detection rate and lower the false positive rate by the advantages of misuse detection and anomaly detection. However, a decision-making module is used to integrate the detect results and to report the types of attacks.

Keywords—Wireless sensor network; Hybrid IDS; Anomaly detection, Misuse detection

I. INTRODUCTION

Advances in wireless communication and miniature electronics have enabled the development of small, low-cost, low-power sensor nodes (SNs) with sensing, computation and communication capabilities. Therefore, the issues of Wireless Sensor Networks (WSNs) have become popular research subjects. WSN is a non-infrastructure network, and through the mass deployment of SNs, a WSN is formed. The major function of WSN is to collect and monitor the related information which about the specific environment. The SNs detect the surrounding environment or the given target and deliver the data to the sink using wireless communication. The data is then analyzed to find out 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. Two of the most common topology of WSN, Flat and Cluster-based Wireless Sensor Network (CWSN) [3], are shown in Figure 1 and Figure 2 respectively.

Because WSNs are composed by numerous low-cost and small devices, and usually deploy to an open and unprotected area, they are vulnerable to various types of attacks. For example, when WSN is applied to the battlefield, SNs are invaded by the enemy and destroyed. Thus, the security of the WSN needs to be considered. A prevention mechanism is used to counteract well-known attacks. It establishes a corresponding prevention method, according to the characteristics of an attack. However, prevention mechanisms cannot resist overall attacks. Therefore, the attacks are required to be detected. An Intrusion Detection System (IDS) is used frequently to detect the packets in a network, and determine whether they are attackers. Additionally, IDS can help to develop the prevention system through acquired natures of attack.

Figure 1. Flat WSN

Figure 2. Cluster-based WSN

The IDS acts as a network monitor or an alarm. It prevents destruction of the system by raising an alarm before the intruder starts to attack. The two major modules of intrusion detection include anomaly detection and misuse detection [6]. Anomaly detection builds a model of normal behavior, and compares the model with detected behavior. Anomaly detection has a high detection rate, but the false positive rate is also high. The misuse detection detects the attack type by comparing the past attack behavior and the current attack behavior. The misuse detection has high accuracy but low detection rate. Especially, the misuse detection cannot detect unknown attacks, which are not in the model base. Many researchers discuss the module of hybrid detection to gain both the advantages of anomaly detection and misuse detection [1,8]. This combination can detect unknown attacks with the high detection rate of
anomaly detection and the high accuracy of misuse detection. The Hybrid Intrusion Detection System (HIDS) achieves the goals of high detection rate and low false positive rate.

In this study, a HIDS is discussed in a heterogeneous CWSN. Cluster head (CH) is one of SNs in the CWSN but the capability of CH is better than other SNs [2]. Additionally, the CH aggregates the sensed data from other SNs in its own cluster. This makes a target for attackers. However, the CH is used to detect the intruders in our proposed HIDS. This not only decreases the consumption of energy, but also efficiently reduces the amount of information. Therefore, the lifetime of WSN can be prolonged.

The remainder of this paper is organized as follows: Section II introduces the common attacks in WSN and the analytic tools of intrusion detection. In Section III, the proposed methods and architecture of our research are introduced. The simulation results used to evaluate the performance of the proposed system are presented in Section IV. Finally, the conclusion and future work is discussed in Section V.

II. RELATED WORK

A. Attacks in WSN

The comparison of attacks in WSN is shown in TABLE I [5,10,11]. However, the majority of attack behavior consists of the route updating misbehavior, which influences data transmission. In the application of CWSN, the data is sensed and collected by SNs, and is delivered to CH to aggregate. The aggregated data is then sent to sink from CH. Therefore, CH is a main target for attack.

<table>
<thead>
<tr>
<th>Attack name</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spoofed, Altered, or Replayed routing information</td>
<td>Route updating misbehavior</td>
</tr>
<tr>
<td>Select forward</td>
<td>Data forwarding misbehavior</td>
</tr>
<tr>
<td>Sinkhole</td>
<td>Route updating misbehavior</td>
</tr>
<tr>
<td>Sybil</td>
<td>Route updating misbehavior</td>
</tr>
<tr>
<td>Wormholes</td>
<td>Route updating misbehavior</td>
</tr>
<tr>
<td>Denial of Service</td>
<td>Data forwarding misbehavior</td>
</tr>
<tr>
<td>Hello floods</td>
<td>Route updating misbehavior</td>
</tr>
<tr>
<td>Acknowledgment spoofing</td>
<td>Route updating misbehavior</td>
</tr>
</tbody>
</table>

B. Analytic Tool of Intrusion Detection

The proposed HIDS in our research not only efficiently detects attack, but also avoids the waste of resources. First, a large number of packet records are filtered by using the anomaly detection module, and then the misuse detection module is used to complete the whole detection. By training the mode of normal behavior, the anomaly detection module detects the normalcy of current behavior, as determined by the rules. The misuse detection module determines if the current behavior is an attack, and the Back Propagation Network (BPN) is used to classify the attacks.

Rule-based presents the thoughts of expert [7]. Because human thought is very complicated, the knowledge could hardly be presented by algorithms. Therefore, a rule-based method is used to analyze results. The rules are defined by an expert, through his experience and observation. Additionally, the rules are logged in a rule base after they have been defined. The basic method of expression of rule is “if…then”, that means if “condition” is established and then the “conclusion” will occur.

Back Propagation Network (BPN) is the most typical and the most general model to use in a neural network [9]. BPN is a model of supervised learning, through the specific environment to get the training data, which includes input and output variables. However, BPN learns from input variables and output variables inherent to the mapping rules to deduce what kind of new input variables, output variables, it is more suitable for diagnosis and prediction, etc.

A network structure of BPN includes many layers, and each layer has several processing units. The network structure of BPN consists of three layers, including an input layer, a hidden layer, an output layer and many links between each layer. The input layer is used to get the outer environmental messages, and by the intersect computing in the hidden layer, a corresponding output is gotten from output layer.

In the progression of BPN training, when all training data have been trained, then the procedure is completed and it is called one epoch. The BPN learns training data repeatedly, and tunes the weights between layers continuously, through many epochs, until the output of the network is similar to the target value and a convergence is achieved.

III. RESEARCH METHOD AND ARCHITECTURE

HIDS proposed in this study consists of three modules is shown in Figure 3. First, the anomaly detection module is used to filter the normal or abnormal packet. Then, the abnormal packets are judged through the misuse detection module for type detection. Finally, the results of the two detection module are integrated by the decision-making module to determine whether the intrusion and the type of intrusion, and return to the manager to follow-up treatment.

As required in CWSN to detect the large number of packets, while the vast majority of packets are normal. As a filter, packets will be screened first by anomaly detection
module. If an abnormal packet is found, then the misuse detection module does further detection. Due to the anomaly detection module in determining whether the intrusion compared with the normal behavior, as if the current behavior and normal behavior patterns vary, the system will be misjudged as abnormal.

In a CWSN, it is necessary for the packets to establish normal patterns of behavior for monitoring the status of packets. Therefore, in this study, the rules-based analysis method is used to build anomaly detection modules and the corresponding rules are defined by experts. The flow of construction can be divided into three steps, as follows:

Step 1: Analysis of network packets sent by the history. In CWSN, the packets, which pass through CH, are sent from: (1) The members of the cluster nodes; (2) The neighbor of CH, which chooses this CH as the transmission path. Therefore, the past packets that communicate on CH are collected to analyze, and the packet is divided into two types of normal and abnormal.

Step 2: Feature selection. Looking for identification of key features issued to distinguish between normal or abnormal packet.

Step 3: The establishment of anomaly detection rules. Based on the definition of a normal packet and the selected features, the rules are created. Then, the well-established rules are stored in the knowledge base.

In the CWSN, when all the SNs communicate with the CH, all the packets through the CH have to be screened by the anomaly detection module, and to be determined whether the abnormal packets. If so, the packets are transferred to the second phase, the misuse detection module is used to detect whether the misjudgment happened or not.

The misuse detection module utilizes various models of well-known attack behaviors, so we should build a model base according to these behaviors. 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. It can make the error for inference be minimal, so as to high accuracy. Therefore, BPN achieves high accuracy for our HIDS through massive trainings. The module is embedded in the SN when BPN has completed the training.

In this research, a three-layer BPN is adopted for our misuse detection module that includes an input layer, a hidden layer and an output layer. We use the abnormal packets, which were determined by anomaly detection module, as the input vector. The number of processing units in input layer is determined through the selected features for packet. In addition, the number of processing units in hidden layer is designed through averaging the input layer units and the output layer units. After analysis, there are eight common attacks exist in WSN, including: Spoofed/Altered/Replayed Routing Information, Select Forward, Sinkhole, Sybil Attack, Wormholes, Denial of Service, Hello Floods and Acknowledgment Spoofing. Nine processing units in the output layer represent eight different attacks and one normal behavior, to determine whether the inputted packet is an intrusion, and make a classification.

The historical records of packet are collected, which pass through CH in CWSN, as the sample data for training. Most of packets are normal in WSN. This makes the training data unbalanced. In other words, the abnormal packets will be neglected by the BPN due to the low occurrence rate. In addition to avoid this problem, the training data is filtered through the anomaly detection module at first, and then the abnormal packets will be left for training.

Before sending the training data to BPN, the training data is normalized into a recognizable form of BPN. In other words, the packet records are converted into a stream binary value, and then be send to BPN. To get a better convergence, the learning rate is set to 0.5 or between 0.1 and 1.0 [9]. The actual learning rate is determined through simulation. Additionally, we assign values between 0 and 1 as the weights and biases randomly. Then, the training data is feed into BPN, computing the actual output through the method of feed forward. The error and correction of output and hidden layers are calculated through the method of back propagation. To update the weights and biases of network, until all training data have been used, this period is called one epoch. The training data can be learned repeatedly and tune the weights between layers continuously, through many epochs, until the output of network is similar to the target value, and the training is complete.

All abnormal packets, which were determined by the anomaly detection module, are subjected to the misuse detection module. First, the abnormal packets are converted into binary value in a preprocessing step, and the binary value is sent into the misuse detection module to calculate the output. Finally, the results of detection are delivered to the decision making module to integrate.

The decision making module is used to integrate anomaly detection and misuse detection module to detect whether the intrusion and the invasion of the type. The module used rules as shown in TABLE II.

<table>
<thead>
<tr>
<th>Rules</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>If anomaly detection module detects an attack and misuse detection module does not detect attack then it is not an attack and it is erroneous classification.</td>
<td></td>
</tr>
<tr>
<td>If anomaly detection module detects an attack and misuse detection module detects attack then it is an attack and determine the class of attack.</td>
<td></td>
</tr>
</tbody>
</table>

### IV. Experiment

In this section, the proposed architecture is evaluated through simulation. However, the corresponding rules in anomaly detection module are defined by experts. Therefore, the correctness is judged by experts. Thus, in the main validation experiments conducted in this study, the use of BPN classification performance of the misuse detection module is evaluated.
A. Data Collection

Due to the real sample cannot be gotten in WSN for intrusion detection; the KDDCup'99 dataset [12] is used as the sample to verify the performance of the misuse detection module. The KDDCup'99 dataset, referred by Columbia University, was arranged from intrusions simulated in a military network environment at the DARPA in 1998. It was performed in the MIT Lincoln Labs, and then announced on the UCI KDD Cup 1999 Archive.

The features consist of 34 types of numerical features and 7 types of symbolic features, according to different properties of attack. Additionally, the KDDCup'99 dataset includes many attack behaviors, classified into four groups: Probe, Dos, U2R, and R2L. It also includes a kind of normal communication. Therefore, these five behaviors for the classification of HIDS are used in the experiment.

The attacks of Spoofed, Altered, or Replayed Routing Information, Sinkhole, Sybil, Wormholes, and Acknowledgment Spoofing, need to make a probe step before they begin to attack, so they would be classified as Probe attacks. Select Forward, which uses illegitimate data forwarding to make attack, is known as a Dos attack. Sinkhole, Wormholes, and Hello Floods are caused by inner attacks, and are therefore classified as U2R. Spoofed, Altered, or Replayed Routing Information, Sinkhole, Sybil, Wormholes, Hello Floods, and Acknowledgment Spoofing, through which the weakness in the system to make attack, so they would be classified as R2L.

In this research, we use the kddcup.data_10_percent.gz as our sample of training and testing dataset in experiment. This includes 10% data in the KDDCup'99 dataset, and the total number of communication records is 494021. It randomly samples 30000 records as training data, and 15000 records as testing data. However, the sample set of Probe, U2R, and R2L is small, hence, the whole records are sampled. Moreover, two-thirds of these records are put as training data, and one-third of these records are put as testing data. While other sample sets are sampled according to their ratio from kddcup.data_10_percent.gz, they are classified to Normal and DoS type separately. The Normal accounts for about 20%, the Dos accounts for about 80%. The data sampling number and ratio are shown in TABLE III.

B. The Simulation Design of BPN

In this subsection, the flow of experiment, feature selection, data preprocessing and the training BPN model are presented.

1) The Flow of Experiment

In this research, we first sample the training and testing data from the KDDCup’99 dataset, and filter some unimportant and noise features to decrease the data dimension. Then, the data are normalized through the preprocessing step, and the data is used to train the BPN model.

2) Feature Selection

Not every feature has decisive effects on the output of classification. Some features even make classification errors. Therefore, feature selection is an important factor to affect the performance of IDS. In this research, the feature selection method proposed by Jong et al. [4] is adopted. Therefore, the data dimensions and the complications can be reduced.

3) Data Preprocessing

Before training BPN model, it must be normalized for the training data, and letting it be a data type which recognizable by BPN. However, the original state is normalized for the training data, and 24 types of features are chosen [4]. To achieve normalization, these 24 features are converted into binary value. We design a corresponding binary value to transfer the original value for the symbolic data. In addition, formula (1) is used to transfer the values into fall between 0 and 1, for the numerical data, and then divide them into several blocks, finally use binary value to replace them.

$$v' = \frac{y - \min}{\max - \min}$$

Additionally, the corresponding target value is classified into 5 groups: Normal, Probe, Dos, U2R, and R2L, which translates to 00001, 00010, 00100, 01000 and 10000, respectively.

4) Training BPN model

BPN is a network model of supervised learning, inputting training data which has target values to make training, learning the training data repeatedly, tuning the weights between layers continuously, until the output of network is similar to the target value, and training is completed. In the training process, original weights and biases are assigned from 0 to 1 randomly. Through the error back propagation to find out the correction, and it would stop until the network gets a convergence. The allocation of each layer in the three-layer BPN is shown below:

5) Input layer: According to the 24 types of features, chosen by Jong [4]. The features are transferred into 95 binary values, and 95 neurons of input layer are produced.

6) Output layer: The outputs have 5 types, including Normal, Probe, Dos, U2R and R2L. Therefore, five neurons of output layer are produced.

7) Hidden layer: Rely on the mean method, adding the number with input units and output units, and dividing it by 2, to get the number of hidden layer unit. The 50 neurons of hidden layer are produced.

C. Simulation Results and Discussion

The adopted system in this research is the AMD Athlon(tm) 64 X2 Dual Core Processor 5000+ 2.59 GHz PC, with 2048MB ram, Windows XP Professional version OS, and using the NNtool which is built-in the MATLAB 7.1 to train the BPN model.
The performance of the experiment is evaluated by the detection rate (DR), the false positive rate (FP) and the accuracy, according to the formulas (2), (3) and (4).

\[ \text{Detection Rate} = \frac{\text{Number of detected attacks}}{\text{Number of attacks}} \times 100\% \quad (2) \]

\[ \text{False Positive Rate} = \frac{\text{Number of misclassified connections}}{\text{Number of normal connections}} \times 100\% \quad (3) \]

\[ \text{Accuracy} = \frac{\text{Number of correct classified connections}}{\text{Number of connections}} \times 100\% \quad (4) \]

According to the result of experiment that shown in TABLE IV, the DR is 99.81\%, the FP is merely 0.57\%, and the accuracy is 99.75\%. To analyze each class of attacks in Table V, to observe each individual performance, the detection performance of the U2R is worst. This is because the training data of U2R are too less, and result in the low detection performance.

TABLE IV. THE PERFORMANCE EVALUATION OF IDS

<table>
<thead>
<tr>
<th>DR</th>
<th>FP</th>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>99.81%</td>
<td>0.57%</td>
<td>99.75%</td>
</tr>
</tbody>
</table>

TABLE V. THE TABLE OF DETAILED CLASSIFICATION

<table>
<thead>
<tr>
<th>Category of attacks</th>
<th>Amount of correct detection /Amount of sample</th>
<th>DR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal</td>
<td>2633/2648</td>
<td>99.43%</td>
</tr>
<tr>
<td>Probe</td>
<td>1358/1369</td>
<td>99.20%</td>
</tr>
<tr>
<td>DoS</td>
<td>10590/10591</td>
<td>99.99%</td>
</tr>
<tr>
<td>U2R</td>
<td>10/17</td>
<td>58.82%</td>
</tr>
<tr>
<td>R2L</td>
<td>366/375</td>
<td>97.00%</td>
</tr>
</tbody>
</table>

V. CONCLUSION AND FUTURE WORK

In our research, HIDS is proposed to detect intrusion by CH of CWSN. The proposed HIDS consists of an anomaly detection module and a misuse detection module. It filters a large number of packet records using the anomaly detection module, and performs a second detection with the misuse detection module when the packet is determined to intrusion. Therefore, it efficiently detects intrusion and avoids the resource waste. Finally, it integrates the outputs of the anomaly detection and misuse detection modules with a decision making module. This determines the presence of an intrusion, and classifies the type of attack. The output of the decision making module 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.

In this paper, the performance of the misuse detection module is evaluated, which is implemented by BPN though experiment. The simulation results present the performance of this method: the detection rate is 99.81\%, the false positive rate is only 0.57\% and its accuracy achieves 99.75\%. We also find that the individual detection rate is very low when the training sample is not substantial. Therefore, the training samples must be a specific amount for the BPN to ensure the accuracy of classification.

The method of feature selection is one of the important factors, which affects the performance of IDS. We adopt the proposed method of feature selection by Jong now, but we can use other methods to select features in the future, such as data mining, to find identifiable features, instead of relying on the viewpoint of experts. Additionally, our rule-based method is also defined by the experiences and observations of experts. We can use a method, which has learning ability, and collocate with the selected features to provide our anomaly detection module with better performance and flexibility.

ACKNOWLEDGMENT

This work was supported in part by the Taiwan National Science Council under Grants NSC97-2221-E-324-007.

REFERENCE


