A Machine Learning Based AIS IDS

Mohammad Mahboubian and Nor Asilah Wati Abdul Hamid, *Member*, *IACSIT*

***Abstract*—In recent years we have seen a very great interest in combining naturally inspired techniques with existing conventional approaches. In this study we combined Negative Selection theory, one of most important theories in AIS, and knowledge production rules to propose a novel IDS. To generate the detectors first we produced a set of basic rules using knowledge production techniques with the help of WEKA, next the new detectors was generated and matured inside negative selection module and the basic rules. After experimenting the proposed model using DARAP 1999 dataset, this model showed a good performance compared to our previous models.**

***Index Terms*—Intrusion detection, artificial immune system, negative selection, data mining, machine learning, WEKA.**

I. Introduction

In recent years, computer science researchers have done great studies in biologically inspired systems and application of these systems in the domain of computer science. The typical biological and natural systems are artificial neural networks, evolutionary computation, DNA computation, and now artificial immune systems (AIS) [1].

AIS is a complicated system with the ability of self-adapting, self-learning, self-organizing, parallel processing and distributed coordinating, and it also has the basic function to distinguish self and non-self and clean non-self.

The problems in the field of computer security and artificial immune systems have the astonishing similarity of keeping the system stable in a continuous changing environment. Artificial immune system can use biological immune theoretic for references to search and design relevant models and algorithms to solve the various problems occurred in the field of computer security [2].

In [3] we proposed a new statistical IDS model based on Artificial Immune System (AIS) whereby in that model the detector sets were chose based on the packet headers and this leads to have system overload and therefore decreasing the overall performance of the model.

Whereby In [4] we proposed a novel hybrid intrusion detection model based on the combination of one of the most important artificial immune system theories namely negative selection as well as a traditional data mining method, i.e. statistical approach with ability of applying vaccine operation where it could detect known attack as well as unknown attacks.

Here in contrast with the work in [3] we did not use clonal selection theory and also our detector sets were all binary detector sets.

Also the proposed model was experimented with a well-known dataset among IDS researchers called DARPA [5].

Although the performance of the model was enhanced in compared with the work in [3] significantly but in some attack categories such as probing the detection rate was not satisfactory therefore in this paper we are combining expert production rules techniques and the previous proposed model in [4] to come out with a better new model in terms of detection rate and also false positive.

The remainder of the paper is organized as follows. First, we describe necessary facts which are required to understand the rest of paper. Next we review the work in [4] as our proposed model is an extension of this work, and then we propose our model. The paper is ended by experimental results of the proposed model as well as discussion.

II. Relative Knowledge

A. Immune System

Natural immune system is a remarkable and complex defense mechanism, and it keeps the organism away from the virus and bacterium and so on. So, as an immune system, the first thing to deal with is that how the cells which to execute immune function(the lymph cells) differentiate organism's self-cells from other cells, in other words, how to insure the lymph cells to take no immune reaction with organism's self-cells. This mechanism is completed via a process known as negative selection of the organism's lymph cells (mainly T-cells and B-cells), which allows only the survival of those cells that do not recognize self-cells [6].

B. Negative Selection Mechanism

The purpose of negative selection is to provide tolerance for self-cells. It deals with the immune system's ability to detect unknown antigens while not reacting to the self-cells. During the generation of T-cells, receptors are made through a pseudo-random genetic rearrangement process. Then, they undergo a censoring process in the thymus, called the negative selection. There, T-cells that react against self-proteins are destroyed; thus, only those that do not bind to self-proteins are allowed to leave the thymus. These matured T-cells then circulate throughout the body to perform immunological functions and protect the body against foreign antigens.

C. Dataset

To assess and evaluate the performance of the proposed algorithm we use the same dataset which previously we used in work [4] MIT Lincoln Lab 1999 off-line intrusion detection evaluation data set [5].We are using the same dataset so that

Manuscript received January 14, 2013; revised May 18, 2013.

The authors are with the Universiti Putra Malaysia, Serdang, 43400 Selangor, Malaysia (e-mail: GS24880@ mutiara.upm.edu.my, asila@fsktm.upm.edu.my).

we can have a fare comparison and better understanding of improvement of the proposed model in compared with the work in [4].

MIT Lincoln Lab 1999 data set includes 5 weeks of data which comprise of 3 weeks of training data (attack free data) and 2 weeks of testing data (with attack data).

There are 201 attack instances embedded in the MIT Lincoln Lab evaluation data set for both inside and outside testing data. Out of 201 attack instances only 176 are found in the inside testing data used for this experiment. Our performance evaluation will be based on the 176 attack instances as we only use the inside testing data.

Table I shows the distribution of all attack categories inside the inside testing data.

TABLE I: SHOWS THE DISTRIBUTION OF ALL ATTACK CATEGORIES

Category	TCP	UDP	ICMP	TOTAL
Probe	30	7	8	45
DOS	37	10	7	54
U2R	54	3	0	57
R2L	4	2	0	6

D. Expert Production Rules

The format of the production rules like other generated rules in the field of artificial intelligence is of form of form of antecedent and consequent. For instance in case of our model these rules are of the following format:

Antecedent
IF some conditions are true
Consequent
Then
The packet is analogues
For example:
IF source IP is anomalous
AND destination Port is greater than n
Then
This packet can be considered as an attack packet.

We will extracts these rules based on the normal profile which we have from the network and applying them with test packets and then we apply these rules for each packets based on its protocol type. Therefore for each of TCP, UDP and ICMP packets we will extract different kind of rules.

All these rules will be used in negative selection module in our model.

III. RELATED WORKS

In this paper our main objective is to enhance our previous work in [4] using expert production rules which is considered a data mining technique. Therefore for better understanding this model first we describe the work in [4] briefly.

In [4] using a biologically inspired approach called AIS (Artificial Immune System) and also a statistical approach which is considered as a conventional data mining and machine learning method we proposed a hybrid intrusion detection system. Fig. 1 shows this model.

One of the most important modules of this model was negative selection module which was responsible for creating different detector sets and sending those matured detector sets to another module.

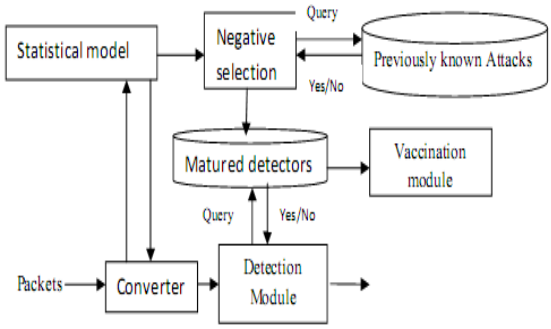

Fig. 1. Our proposed model in [2].

The way that this module work is as follow:

First it created a random binary set based on packet header fields in Table II for one of the TCP, UDP or ICMP protocols.

Then for each newly created packer it calculates the anomaly score. Finally If the anomaly score for that particular set was below some predefined threshold that set was thrown away because it is considered as self, but if the anomaly score was above the threshold value then that particular set was considered as non-self and was added into the matured detector repository.

TABLE II: THE PACKET HEADER FIELD USED TO PRODUCE NORMAL PROFILE

TCP	UDP	ICMP
Source IP	Source IP	Source IP
Dest. IP	Dest. IP	Dest. Port
IPFragID	IPFragID	IPFragID
IPFragOff	IPFragOff	IPFragOff
TCPSeq.	Source Port	
TCPAck.	Dest. Port	
Source Port	UDP Length	
Dest. Port		

Although the detection rate in this model was quiet satisfactory and interesting but for some categories of attacks the detection rate was not so much satisfactory. We also intended to decrease the false positive of this model therefore we proposed a new model whereby in this model our focus is more on the negative selection module.

IV. PROPOSED MODEL

A. Model Details

In this model we replace the negative selection module in our previous model in [2] with a new one. In the new negative selection module instead of using only normal profile to distinguish and classified packets into two different classes of 'Normal' and 'Anomaly', we do future process on each packet using our expert rules, produced before based on the normal profile table. This way each packet should undergo more stages in order to find out if it is an anomalous packet and as a

result the false positive rate of our model is decreased significantly, its detection rate is increased.

B. Experimenting the Model

In order to generate expert production rules in this paper we used a tool called WEKA [7] which is a very powerful and stable open source machine learning tool. WEKA also has more than 80 classifier algorithms to do the rule extraction and in this paper according to [8] we chose J48 Tree classifier algorithm which seems to be the best classifier algorithm based on our dataset. After creating the tree then using WEKA it is very easy to generate and extract production rules.

Each leaf of this tree can be considered as a new expert rule.

Following are the steps involved in generating this tree:

First we need to select one of the hosts in our dataset with the most attacks on it and after generating the rules we generalize our rules so that they can be applied on the rest of host in our model.

So for a particular host we need to create normal profile. Then we filter all the packets which is coming out from this host or going in to this host and also based on the particular protocol. Therefore at the end we came up with 3 tables of TCP, UDP and ICMP packet header for this particular host.

The next step is to identify which packet in the testing Dataset is an attack and which one is a normal packet. Basically this is done using the list of actual attacks provided by the DARPA IDS Dataset.

The last step is to let WEKA to process the final tables for each of TCP, UDP and ICMP protocols.

Here we have to mention that because the behavior of packets coming to a host and going out from a host may change (for example due to changes in behavior of the user who uses that host) we need to repeat the procedure of extracting the expert rules on a periodic basis. This way we ensure that our false alarm rate is kept low.

```
Time taken to build model: 0.33 seconds

=== Stratified cross-validation ===
=== Summary ===

Correctly Classified Instances       35021               100      %
Incorrectly Classified Instances         0                 0      %
Kappa statistic                          1
Mean absolute error                      0
Root mean squared error                  0
Relative absolute error                  0      %
Root relative squared error              0      %
Total Number of Instances            35021

=== Detailed Accuracy By Class ===

               TP Rate   FP Rate   Precision   Recall  F-Measure   ROC Area  Class
                 1         0          1         1         1          1        Normal
                 1         0          1         1         1          1        probe
                 1         0          1         1         1          1        dos
Weighted Avg.    1         0          1         1         1          1

=== Confusion Matrix ===

     a     b     c   <-- classified as
 32895     0     0 |     a = Normal
     0  1990     0 |     b = probe
     0     0   136 |     c = dos
```

Fig. 2. The output from WEKA for UDP protocol and only for one particular host.

For example here is one of the UDP rules extracted from the dataset:

Antecedent

IF source IP is anomalous AND UDP destination port AND UDP Source Port are < 1024

Consequent

THEN packet is a DOS attack.

Fig. 2 and Fig. 3 show our experiment with WEKA for a particular host and UDP protocol.

The tree in Fig. 3 is the result of the classification done by WEKA which is then converted to the expert rules and each leaf is a rule.

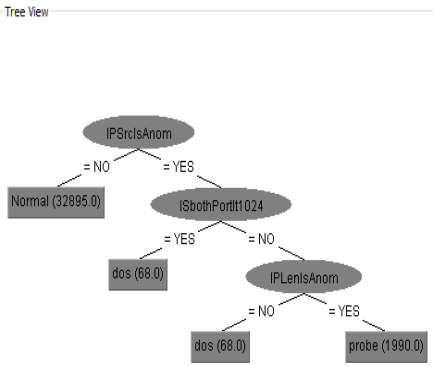

Fig. 3. The output tree generated for UDP packet which is only for a particular host.

V. Conclusion and Future Work

After conducting the experience it was shown that the overall performance of our new model in terms of false positive and detection rate is better than the previous model in [4].

However this enhancement was surprisingly more significant on some attacks categories than the others.

Table III shows the performance of our model in term of detection rate for different categories of attack inside our dataset.

TABLE III: The Experimental Result Using Expert Rules

Attach Category	Work in [4]	The Proposed Model
Probe	91.32%	92.59%
DOS	73.98%	75.02%
U2R	62.63%	66.87%
R2L	58.45%	63.39%

Table III shows that after replacing the negative selection module in our model with the new one built from expert rules we actually can increase the performance of previous work [4] in term of decreasing false positive. From this we can conclude that either utilizing negative selection in intrusion detection systems may leads to high rate of wrong detection or if the algorithm used in negative selection should be chosen carefully.

In this paper the main focus of our proposed model was detecting some particular categories of attacks therefore as one of our future work we intend to enhance our new propose model to increase its detection rate range so that we can detect more categories of attacks.

Also we are interested in experiencing our proposed model with more realistic datasets or even testing it in a real situation like university network campus.

REFERENCES

[1] B. Mykejee, L. T. Heberlein, and K. N. Levitt, "Network intrusion detection," *IEEE Network*, vol. 3, pp. 26–41, 1994.

[2] U. Aickelin, P. Bentley, and J. McLeod, "Danger theory: the link between AIS and IDS," in *Proc. ICARIS-2003, 2nd International Conf. on Artificial Immune Systems*, 2003, pp. 147–155.

[3] M. Mahboubian and N. A. W. A. Hamid, "A novel intrusion detection model based on combination of artificial immune system and data mining approaches,'' in *Proc. WEC-2010, 4th World Engineering Congress*, Malaysia, 2010.

[4] M. Mahboubian and N. A. W. A. Hamid, "A naturally inspired statistical intrusion detection model," in *Proc. of ICINC 2010*, Malaysia, 2010.

[5] MIT Lincoln laboratory 1999 darpa intrusion detection data sets (1999). [Online]. Available: http://www.ll.mit.edu/IST/ideval/data/1999/1999_data_index.html

[6] S. R. Duan and X. Li, "The anomaly intrusion detection based on immune negative selection algorithm," in *Proc. IEEE International Conference on Granular Computing* 2009, *GRC '09*, 2009.

[7] *WEKA, Software. Machine Learning*. The University of Waikato, Hamilton, New Zealand. [Online]. Available: http://www.cs.waikato.ac.nz/ml/weka/

[8] S. B. Shamsuddin, "Applying knowledge discovery in database techniques in modeling packet header anomaly intrusion detection systems," *Journal of Software*, vol. 3, no. 9, December 2008.

M. Mahboubian was born in Tehran, Iran in 1979. He received his B.Eng. degree in Electronic engineering from Islamic Azad University of Qazvin, Iran in 2004 and Master of Computer Science from university of Pune, India in 2006. He is finishing his Ph.D. in Computer networks and security by end of this year from University Putra Malaysia, Kuala Lumpur, Malaysia. Some of his research interests are computer security and specially intrusion detection systems, artificial immune systems and machine learning.

N. A. Wati Abdul Hamid is a visiting scholar at High Performance Computing Lab, George Washington University, Virginia Campus, USA. She is also a senior lecturer at the Department of Communication Technology and Network, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, Malaysia. She received her Ph.D. from University of Adelaide in 2008. Her research interests are in parallel and distributed computing, cluster computing and other applications of high-performance computing. She is also an associate researcher of High Speed Machine at Institute for Mathematical Research (INSPEM), Universiti Putra Malaysia. She is an IEEE member since 2006.