A Naturally Inspired Statistical Intrusion Detection Model

M. Mahboubian and Nor I. Udzir, *Member*, *IACSIT*

***Abstract*—Growing interest in computational models based on natural phenomena with biologically inspired techniques in recent years have been tangible. The use of immune mechanisms in intrusion detection is promising. In [1] we proposed a new IDS model based on the Artificial Immune System (AIS) and a statistical approach. In this paper we are going to enhance that model in terms of detection speed and detection rate as well as overall overload. In contrast with the work in [1] here we do not use the concept of clonal selection and we use binary detector sets which leads to lower overload and therefore higher performance. The model is examined with DARPA data set which is famous among IDS researchers.**

***Index Terms*—Intrusion detection, artificial immune system, negative selection, data mining, network security.**

I. Introduction

In the last few years, researchers have shown great interest in studying biologically inspired systems in the domain of computer science, sociology, and so on. Among these, computer science has made significant advances with biologically inspired theories fitted in every branch. The typical bio-inspired systems are artificial neural networks, evolutionary computation, DNA computation, and now artificial immune systems (AIS) [2].

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. [3]

In [1] we proposed a new statistical IDS model based on Artificial Immune System (AIS) whereby in that model the detector sets were based on packet headers and this caused to higher overload and decreasing the overall performance of the model.

In this paper we propose 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 can detect known attack as well as unknown attacks.
Here in contrast with the work in [1] we do not use clonal selection theory and also our detector sets are all binary detector sets.

Also the proposed model will be experimented with a well-known dataset among IDS researchers called DARPA [7].

The inspiration behind our proposed model and specially its data mining part is taken from a work in [4] whereby in their model they used TCP, UDP and ICMP packet header field values to learn the anomalous behavior of the packets during transmission in any TCP/IP network traffic.

Using the result of this work and combining it with artificial immune system this paper proposes a novel Hybrid IDS model with the capability of applying vaccine based on detected seen and unseen attacks.

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 describe the work in [4] as part of our model is an extension of this work, and then we propose our model and the way we have implemented it. The paper is ended by result of the experience and future work of our model.

Manuscript received November 9, 2012; revised December 18, 2012.

The authors are with Faculty of Computer Science and Information Technology University Putra Malaysia, Kuala Lumpur, Malaysia (e-mail: Mahboubian.uni@gmail.com, izura@fsktm.upm.edu.my).

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. [5]

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. Detector Set

Basically our detection method is based on comparing each packet with our detector sets and if we find out a packet is similar to one of our detector sets that packet is considered as attack. Figure 1 shows the typical format of detector sets.

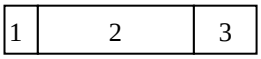

Fig. 1. Format of detector set.

Each detector set has 3 binary parts:

- Protocol type which defines the current detector set is for which protocol TCP, UDP or ICMP
- The Signature of that detector set which will be created during negative selection procedure
- The Vaccine for that set which is applied after detecting an attack

D. Vaccine

A vaccine in this model is basically a kind of response to the detected attack. This response can be creating a new rule in the firewall to block a particular IP address or to close a specific port number in a host inside the network. All the existing responses are mapped to a particular binary number and are defined by the network administrator before running the model.

E. Dataset

To assess and evaluate the performance of the proposed algorithm we used MIT Lincoln Lab 1999 off-line intrusion detection evaluation data set [7] as this data set has become one of the *de facto* standards for test data set among the IDS researcher community.

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

III. PROPOSED MODEL

A. Introduction

As part of our proposed model which is related to data mining has inspired and extended from the work in [4] therefore before we can illustrate our proposed model it is necessary to explain this work briefly and then we proposed our model.

The proposed statistical IDS model in [4] for each of TCP,UDP and ICMP protocols , researchers indexed each header field as i, i=1,2,…,n, so their model is built based on the ratio of the normal number of distinct field values in the training data, Ri, against the total number of packets associated with each protocol, Ni. The ratio, pi = Ri/Ni represents the probability of the network seeing normal field values in a packet. Thus, the probability of anomalies will be 1- pi for each corresponding field. Each packet header field containing values not found in the normal profile will be assigned a score of 1 – pi and will be summed up to give the total value for that particular packet.

At the end if the total scores for a particular packet is more that some threshold that packet considered as an anomalous packet.

$$Score_{packet} = \sum_{i=1}^{n} (1 - p_i) \quad , \; i = 1, 2, \ldots, n \tag{1}$$

As one of the result of this work, it has been mentioned that the effect of some of the header fields in detecting the attacks are very prominent in compared with the rest.

B. Our Proposed Model

Figure 2 shows our proposed model. There are different modules in this model and each one has its own responsibilities. The following is description of different modules which exist in this model.

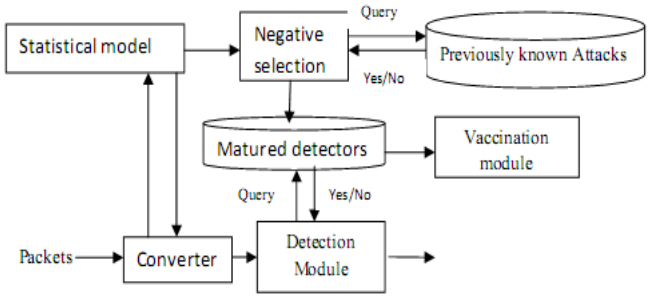

Fig. 2. Proposed model

- Statistical Model: in this module, first based on the normal data (the data without attack) that we have and with inspiration from the work in [4] we create a normal statistical model and then according the equation 1 the anomaly score for each field is calculated.

Here in contrast with the work in [4] which uses all the header fields we only use the most effective packet headers to create our normal statistical model Table II shows the selected header fields.

TABLE II: SELECTED HEADER FIELDS FOR CREATING NORMAL STATISTICAL MODEL.

Protocol	TCP	UDP	ICMP
Selected Fields	Source IP	Source IP	Source IP
	Dest. IP	Dest IP	Dest. IP
	Ipfragid	Ipfragid	ipfragid
	IPfragptr	IPfragptr	IPfragptr
	TCPSeq	UDPSrcPort	
	TCPack	UDPDestPort	
	TCPSrcPort	UDPLen	
	TCPDestPort		

- Negative Selection Module: This module is responsible for creating different detector sets and sending the matured detector sets into another module which is called detector sets repository. Negative Selection module works as follow:

Creating a random binary set based on packet header fields in Table 1 for one of the TCP, UDP or ICMP protocols.

Calculating the anomaly score for that particular newly created set.

If the anomaly score for that particular set is below some fixed threshold that set will be omitted because it is considered as self, but if the anomaly score is above the threshold value then that particular set is considered as non-self and will be added into the matured detector repository.

- Vaccination Module: After detecting an attack, the vaccine section of the detector set which recognized this attack will be checked for any vaccine (Response to the attack) if there is any, and that vaccine will be applied to the network by vaccination module.
- Converter Module: Before processing each packet it should be converted to a binary format so that we can compare that packet against our detector sets (detector sets are also in binary format).This process is done by connecting to the statistical model to see which packet headers inside the packet is not seen previously.

C. Experimenting the Model

This section describes the implementation stages involved in this research:

Reproducing the statistical model used in [4]:

To show that our proposed model enhances the work in [4], firstly we need to re-build the statistical model which is used in [4]. However we do not use all of the packet header fields they used and we only use the most effective ones according to authors in [4] which are shown in Table 1. This leads to speed up the process of detection and to increase the overall performance of the model. Following are steps that have been done to reproduce the model in [4]:

- Writing a program to convert our training data set from TCP-dump format to CSV format and then inserting them into SQL- server database.
- Counting the number of distinct values for each of chosen packet header fields and then producing normal profile table for each of TCP, UDP and ICMP protocols.

D. Building Negative Selection Module

During this stage we should be able to create our detector sets based on the result from stage one. For this stage we need to write another program to generate a random binary set based on the header fields that we have selected.

In this set if we want to introduce a header field as an anomalous filed we should set it to 1 and otherwise the value of a bit is 0.

Referring to Table 1 a TCP type detector set signature can be look like as below:

00000001

Fig. 3. A sample tcp packet signature

Which means in this set only TCP destination port is anomalous, which means its value has not been seen in the normal data previously. Note that this is only the signature part of the detector set and to build a complete detector set two more information should be added to this binary array which are type of protocol (should be added at the first) and vaccine (which should be added at the end of this binary array).

After generating each new set the anomaly score of that set will be calculated based on the normal profile created in stage one. If the score is below some predefined threshold that detector set considered as self and will be removed automatically. If the score is above the threshold that packet will be added to detector set pool which is called Matured Detectors Module.

E. Anomaly Detection

In this stage the model is experimented against the testing data which are taken from our chosen dataset.

Following are steps included in this stage:

- Each testing packet will be compared against the matured detector set module. If there is a similar packet inside the detector set this packet is considered as an attack.
- After detecting an attack, the detector set which helped us to detect the attack will be checked for any vaccine (response to attack), if there is a vaccine in that set, another module which is called vaccination module, applies the vaccine to the network or the host under the attack.

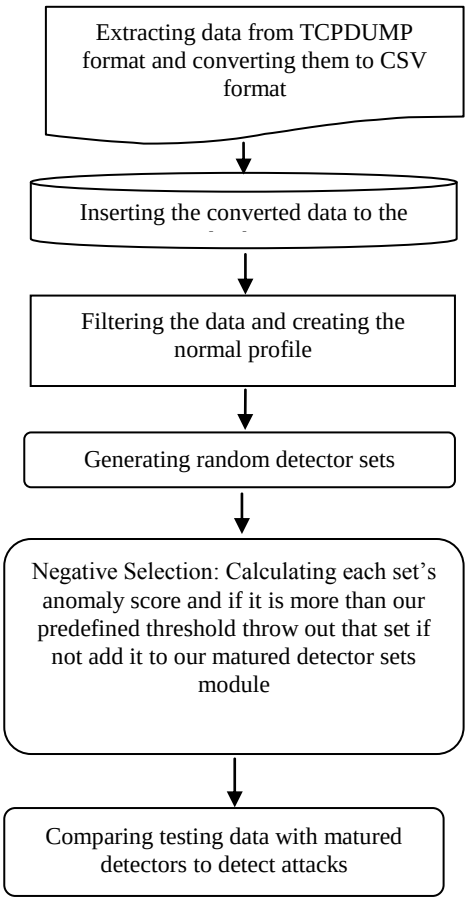

Fig. 4. Proposed model process flow

- A signature regarding to the detected packet will be added to the previously known attack module which is another module of our model, if the attack is considered a new attack (unseen attack), so that we can detect the similar

attacks later quickly.

IV. Experimental Results and Future Work

After conducting the experience we found that our model performance in term of overhead and detection speed is better than the work in [4] and this is because of using less and most effective packet headers in our model. Also the experience shows that the detection rate of our model is higher the detection rate of the work in [4].

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

TABLE III: The Arrangement of Channels

Attach Category	Work in [4]	Our Model
Probe	86.67%	91.32%
DOS	68.52%	73.98%
U2R	59.26%	62.63%
R2L	49.12%	58.45%

As it can be seen from Table III our proposed model can increase the performance of the work in [4] both terms of system overhead and speed as well as detection rate.

In term of false positive also our model performance is better that the work in [4] but because their difference is not satisfactory one of our future goal is to increase the performance of our model in term of false positive. We also intend to repeat the same experiment using other data set such as "capture the flag 2010" dataset [8] and also real network traffic.

References

[1] 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.

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

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

[4] S. B. Shamsuddin and M. E. Woodward, "Modeling protocol based packet header anomaly detector for network and host intrusion detection systems," F. Bao et al. (Eds.): CANS 2007, LNCS 4856, pp. 209–227, 2007. © Springer-Verlag Berlin Heidelberg, 2007.

[5] 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.

[6] D. Dasgupta "Artificial immune systems and their applications," Springer Verlag, 1999.

[7] 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

[8] Capture the flag traffic dump. [Online]. Available: http://www.defcon.org/html/links/dc-ctf.html.