International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 5 2622 – 2625

Enhancing the Security of a Network System using Liquid State Machine- A Novel Approach

Ms. Rucha P. Joshi
Department of Computer Engg.
D.Y. Patil College of Engineering, Akurdi
Pune, India
Email: rucha.joshi390@gmail.com

Mrs. Shanthi K. Guru.
Department of Computer Engg.
D.Y. Patil College of Engineering, Akurdi
Pune, India
Email: gurushaanguru@gmail.com

Abstract- Today, most of the computer applications are network based and there is a steady grow in terms of its size and demand. To keep pace with its security aspects lot of techniques are used like IDS (Intrusion Detection System), anti-virus system etc. All are performing their jobs quite well but produced high volume alarms or messages. Further they are not able to unify the network. Hence to overcome these problems we recommend the use of network security situation assessment method. This paper starts with the discussion of network related security situation concept and proceeds with two concern techniques like SVM (Support Vector Machine) and ESN (Echo State Network) which are discussed in detail. Further we also compare both techniques in terms of their performances. Finally we proposed the application of LSM (Liquid State Machine) to enhance the overall performance of network system.

Keywords— *Intrusion Detection System, Anti-virus System, Network Security Situation Assessment, Support Vector Machine, Echo State Network, Liquid State Machine and Spiking Neural Network .*

*****

I. INTRODUCTION

The aim of network security situation is to know the current status of network system. And it can also perform this task dynamically. It has been observed that it becomes most favourite in field of network security [1]. As today each organization has its own network, they are trying to keep both the information and the information system secured. Hence as a result there is an increase in overall complexity of the network. Lots of conventional security solutions are used to complete the task of ensuring network security. Prominent among them are VPN (Virtual Private Network), IDS (Intrusion Detection System), Anti-virus system and so on. These tools are widely used in the world. Each of these tools separately performs their tasks of establishing the security of the network by generating various kinds of messages or security alarms. More over these security alarms are high in volume and created on daily basis. Therefore it becomes difficult for network administrators to seek overall optimality. Also when network increases in size and weight things becomes worst. To reduce the burden of security management activities and to provide security to networked systems in an efficient manner we emphasis the use of network related security situation. It has the ability to unify whole network. Consequently helps to determine security policies for the network. Further it can predict evolution trend in dynamic environment. All these features greatly help network administrators in monitoring the network and also assist them in decision-making functions. Hence an effective tool on network security situation awareness is highly required to help us fuse all available information properly and comprehend the situations of network security with ease.

This paper discusses two techniques related to network security situation. First is SVM[2] which is a Support Regressions Machine widely used in the classification and regressions problems and second is the ESN[3] which is Echo State Network used as computational construct like neural network; it consists of large collections of units called neurons. If applied properly this construct gives results in timely and accurate manner and thus helps network administrator in analyzing security related situation. We compare & analyze the performance of each and arrived on the result that both SVM and ESN are better and in some cases ESN is far better than the rest in terms of accuracy of network security situation. However each of these has some limitations. Like the training speed of SVM algorithm is slow when the training sample is too large or ESN can't handle continuous time input signals which is a major drawback in large networks. To overcome these limitations we proposed an application of LSM (Liquid State Machine)[4]. LSM which is same as ESN computationally more powerful and is able to react non-linearly to individually timed inputs. Unlike ESN which can't handle continuous time input signals; LSM can handle continuous time inputs naturally. And also computations on various time scales can be done using the same network.

II. RELATED WORK

The term network security situation was conceived by Tim Bass [5] which refers to the operational representation that merge all available information to categorize attacks and awareness of it leads to pick and apply proper countermeasures. Network security situation awareness system keeps records of the various types of information such as logs, alerts of the different network security devices, should have the ability to hold information coming from multiple sources, also include the information of network topology, network composition, vulnerabilities and etc. Based on apt information synthesis, such system gives network analysts the handy approach into the security related activities occurring within their networks, so as to

 ISSN: 2321-8169
2622 – 2625

help them make choice or adaptation in their networks. This system should not only observe the transformation of network situations in real time, but could be react to it precisely, and also present the situations of network security in a competent way.

There are numerous system equipment currently used in the field of network security situation awareness, such as VisFlowConnect-IP[6] and NVisionIP[7]. Most of these exercises flow traffic to offer network security situation information. For example, the tool NVisionIP graphically shows the relations and the traffic flows among hosts in a class-B network to let analyst understand the recent state of the network. The tool VisFlowConnect-IP envisage IP network traffic flow dynamics to supply a general view of the entire network, which permit network analyst to visually measure the connectivity of large and complex networks. So far these tools illustrate outcome in graphics form for this reason not work fine particularly when network connection is slow. Other efforts incorporate systems like Security Situation Analysis and Prediction System for Large-scale Network (SSAP) [8] or Comprehensive Network Security Situation Awareness System (CNSSA) [9]. However, both the systems work well for large-scale network & it is complex and difficult to build up the classification model with the Markov method. So we proposed techniques like SVM and ESN. SVM was proposed in 1992 by Vapnik, et al. At present, it is commonly used in the classification and regression problems [2]. It is stand on the statistical VC theory. It is relatively easy to train and seek the overall optimality. It is convenient to transform to high-dimensional data. Its performance is significant in balancing the complexity and error of the classification. Because SVM can control it very directly. While ESN algorithm was proposed by H. Jaeger of Germany Jacobs University in 2001[3]. It has a Dynamic Reservoir (DR) which is builded by numerous neurons. Its training algorithm is exceptionally simple and efficient. Contrast to SVM, ESN is a novel supervised learning method as a kind of recurrent neural networks (RNNs).Compared with other traditional algorithm an ESN has high accuracy and powerful capability in approximating nonlinear dynamic system.

III. IMPLEMENTATION DETAILS

A. Design

The proposed architecture is shown in fig. 1 given below. It contains components like packet inputs, select rules, apply SVM/ESN/LSM & classification. We can apply any of these techniques alternatively to perform classification. Output is obtained in form of classification file which gives details of normal packet & attacked packet.

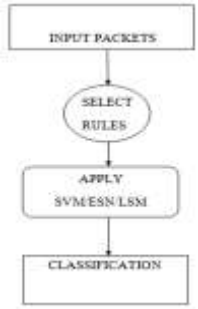

Fig. 1 Proposed System Architecture

B. How does SVM and ESN *works?*

Both SVM *and* ESN uses training and testing method for classification of normal and attacked packets. Fig. 2 shows this classification model.

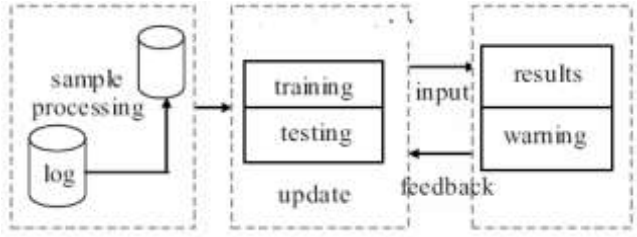

Fig. 2 Classification Model of System

The classification model takes log of input packets. Packets are collected in range from hundreds to thousands. From these input it generates results in form of classification file which includes details of normal and attacked packets. It provides warning messages which can be applied as a feedback to the model.

C. Proposed Work

The LSM is a novel approach towards computation. It uses the internal dynamics of a recurrent Spiking
Neural Network (SNN) to carry out computations on its input. The internal state of the SNN (called the liquid) serves as a input for readout function. The liquid itself does not generate any output; it merely serves as a 'reservoir' for the inputs. The readout then looks at the liquid state (the response of the liquid to a certain input), and computes the output of the LSM. An analogy (and also an explanation for the name Liquid State Machine) can be found in a real liquid as shown in Fig. 3 which consists of a collection of elements that exert an influence on their immediate neighbours. And, like in the case of the LSM, external stimuli or 'inputs' - e.g. a stone that is thrown into a pond - remain detectable for a long time after they have started - like ripples on the same pond. The inputs and outputs of LSMs are arrays of time series. Comparing to Turing computation, this model facilitates the analysis of continuous streams of input. Given a time series of input, the machine can produce a time series of behaviours as output [10]. The main goal of this paper is to show how well Liquid State Machines can be used for recognizing temporal patterns in noisy continuous input streams. It has been also observed that the Liquid State Machine model has a near-identical twin: the Echo State Machine.

Fig. 3 An Analogy for Liquid State Machine

ISSN: 2321-8169
2622 – 2625

D. Algorithm
The steps are as follows:

1. Initially packet inputs are divided into two parts for training & testing. Training is used to train the work presented while test dataset is used to test it.
2. Start with collecting packet inputs.
3. Apply SVM/ESN/LSM. We assume three layers like input units, dynamic reservoir & output units.
4. Generate classification file as output.

E. Mathematical Model
System contains three layers like input units, dynamic reservoir & output units. They are represented as follows.

1. $U = (u_l (n), u_2 (n), \ldots , u_K (n))$
2. $X = (x_1 (n), x_2 (n),. . . .., x_N (n))$ and
3. $Y = (Y_1 (n), Y_2 (n)... Y_L (n))$.
4. The weight matrix of input is Win;
5. of the dynamic reservoir is W; of output is W_{out} and of
6. Feedback is W_f .

The internal state updating equation and output classification equation of DR are listed as follows:
$x (n+ 1) = f (W_{in} u (n+1) + W x (n) + W f_y (n))$
$y (n+1) = f_{out} (W_{out} (u (n+1), x (n + 1), y (n)))$

IV. EXPERIMENTAL RESULTS AND ANALYSIS

For implementation purpose we make use of Eclipse IDE and Java language. It can capture data packets dynamically as well as efficiently. Fig. 4 shows results which describes normal and attacked packets. We measured the Mean Square Error (MSE) and Mean Absolute Percentage Error (MAPE) of all the techniques and captured it in the form of graphs as shown in fig. 5 and fig. 6 respectively.

Fig. 4 Results of Classification

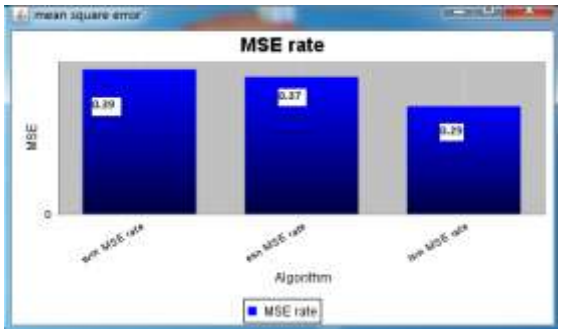

Fig. 5 MSE Rate

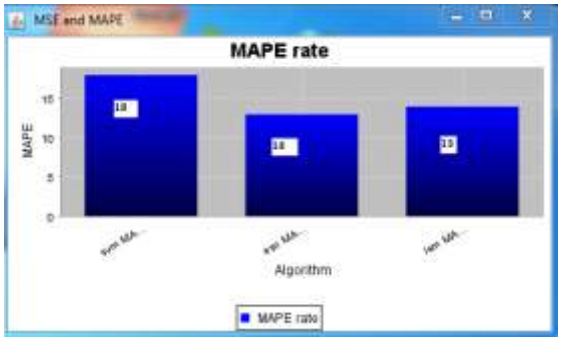

Fig. 6 MAPE Rate

By observations based on the given graphs we must say that LSM is far better than ESN and SVM in terms of performance. It is important to note that this experimental setup shows drawbacks of both of these techniques; particularly the training speed of SVM algorithm is slow when the training sample is too large or ESN can't handle continuous time input signals.

V. CONCLUSION

With tremendous attacks on the network there is a high demand for network analysts to know about the situations of network security effectively. Various systems, techniques & tools are studied. This leads to proposed work of application of the LSM. LSM is not only removes the drawbacks of SVM and ESN but also much efficient, can apply on any size of the network and thus enhance the security quite well.

ACKNOWLEDGMENT

With many thanks to my guide as well as co author of this paper Mrs. Shanthi K. Guru for her never ending encouragement and patience. I am obliged for the suggestions made by my all friends. As always, my gratitude goes to my parents, Mr. Prakash S. Joshi & Mrs. Godavari P. Joshi for their vigorous support. Finally, the one who figure my career is my sister Ms. Y. P. Joshi whose gratefulness can't be expressed in words.

REFERENCES

[1] Shan Yao et. al., "A network security situation analysis framework based on information fusion," third IEEE international conference, pp.326-332, 2011.

[2] Xiaorong Cheng and Su Lang, "Research on network security situation assessment and prediction," fourth international conference on digital manufacturing and automation, pp.1565-1569, 2012.

[3] Fenglan Chen, Yongjun Shen, Guidong Zhang and Xin Liu, "The network security situation predicting technology based on the small world echo state network," IEEE international workshop, pp.377-380, 2013.

[4] Maass W., Natschlager T., et. al., "Real-time computer without stable states: a new framework for neural computation based on perturbations," 2002.

[5] T. Bass, "Intrusion detection systems and multisensor data fusion: creating cyberspace situational awareness," communications of the ACM, pp. 99 -105, 2000.

[6] Slagell A. et.al. "The design of VisFlowConnect IP: a link analysis system for IP security situation awareness," third IEEE international workshop on information assurance, pp. 141-153, 2005.

[7] Kiran Lakkaraju et.al. "NVisionIP: netflow visualizations of system state for security situational awareness," third international conference on network security, ACM publication, 2004.

[8] WeiHong Han, QingGuangWang, "Security situation analysis and prediction system for large scale network SSAP," seventh international conference on computing and convergence technology, pp.1125-1129, 2012.

[9] Rongrong-Xi, Shuyuan-Jin, Xiaochun-Yun, Yongzheng-Zhang, "CNSSA- a comprehensive network security situation awareness system," international joint conference of IEEE trustcom, 2011.

[10] Maass W. & Zador A.M., "Dynamic stochastic synapse as computational units, neural computation," vol.11, pp.903-917, 1999.