ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 2, Issue 2, pp: (27-32), Month: May - August 2015, Available at: www.noveltyjournals.com

INTRUSION DETECTION SYSTEM TO IMPROVE THE DETECTION RATE USING ART-1 ALGORITHM

[1]Akshay Saxena, [2]Anshuman Sharma

Abstract: **Computer networking has become an important infrastructure for our daily communication as it is interconnecting people together to make a borderless world. The usage of internet has increased in various fields like online banking, business tradition, online shopping and so on. Along with that hacking tools are appearing which exploits system vulnerabilities. So computer network security has become very important in order to develop a mechanism that provides a defense against the intrusions from attackers. Thus Intrusion Detection System (IDS) acts as a second line important component of the defense-in depth security mechanism. To detect the attack with the great accuracy is our major concerned. Many neural network (NNs) techniques have been used for detection of the attacks. This paper analyzes different Adaptive Resonance Theory (ART) techniques that are being used in IDS to detect attacks. Among those Fuzzy ART technique has been found beneficial. This thesis also shows that how different parameters of ART techniques affect the overall performance of the system.**

Keywords: **Intrusion detection system, neural network, false alarm.**

1. INTRODUCTION

An intrusion detection system (IDS) is a component of the information security framework. Its main goal is to differentiate between normal activities of the system and behavior that can be classified as suspicious or intrusive [1]. The goal of intrusion detection is to build a system which would automatically scan network activity and detect such intrusion attacks. Once an attack is detected, the system administrator can be informed who can take appropriate action to deal with the intrusion.

IDS can be host-based (HIDS), network based (NIDS) or a combination of both types (Hybrid Intrusion Detection System). HIDS usually observes logs or system –calls on a single host, while a NIDS typically monitors traffic flows and Network packets on a network segment, and thus observes multiple hosts simultaneously. Generally, one deal with very large volumes of network data, and thus it is difficult and tiresome to classify them manually in order to detect a possible intrusion. One can obtain labelled data by Simulating intrusions, but this will be limited only to the set of known attacks. Therefore, new types of attacks that may occur in future cannot be handled, if those were not part of the training data. Even with manual classification, we are still limited to identifying only the known (at classification time) types of attacks, thus restricting our detection system to identifying only those types. To solve these difficulties, we need a technique for detecting intrusions when our training data is unlabeled, as well as for detecting new and un-known types of intrusions. A method that offers promise in this task is anomaly detection. Anomaly detection detects anomalies in the data (i.e. data instances in the data that deviate from normal or regular ones). It also allows us to detect new types of intrusions, because these new types will, by assumption, be deviations from the normal network usage. It is very difficult, if not impossible, to detect malicious intent of someone who is authorized to use the network and who uses it in a seemingly legitimate way. For example, there is probably no highly reliable way to know whether someone who correctly logged into a system is the intended user of that system, or if the password was stolen.

Under these assumptions we built a system which created clusters from its input data, then automatically labelled clusters as containing either normal or anomalous data instances, and finally used these clusters to classify network data instances as either normal or anomalous. Both the training and testing was done using 10% KDDCup'99 data [2], which is a very popular and widely used intrusion attack dataset. Most clustering techniques assume a well defined distinction between the clusters so that each pattern can only belong to one cluster at a time[18,19]. This supposition can neglect the natural ability of objects existing in multiple clusters. For this reason and with the aid of fuzzy logic, fuzzy clustering can be employed to overcome the weakness. The membership of a pattern in a given cluster can vary between 0 and 1. In this model a data object belongs to the cluster where it has the highest membership value. In this paper we aim to propose a Neural Network based algorithm which is capable finding unseen attack and identify new attack.

2. RELATED WORK

Security in IDS is one of the major areas of research. The survey shows that, the researchers are focusing on efficient algorithms and encryption techniques to enhance the data security in IDS.

Brian Hay et. al [6] have focused on data authentication, data integrity, querying and outsourcing the encrypted data. Their research says that, the risks can arise at operational trust modes, resource sharing, new attack strategies and digital forensics. In operational trust modes, the encrypted communication channels are used for cloud storage and do the computation on encrypted data which is called as homomorphic encryption. New attack strategies like Virtual Machine Introspection (VMI) can be used at virtualization layer to process and alter the data. The issues are clarified using the digital forensics techniques namely the ephemeral nature of cloud resources and seizing a "system" for examination.

John C. Mace et.al [7] have proposed an automated dynamic and policy-driven approach to choose where to run workflow instances and store data while providing audit data to verify policy compliance and avoid prosecution. They also suggest an automated tool to quantify information security policy implications to help policy-makers form more justifiable and financially beneficial security policy decisions. Service oriented architecture (SOA) is used for work flow deployment in an enterprise. For efficiency, productivity and to achieve public cloud, the cloud computing uses the approaches like retaining control, setting policy, monitoring and runtime security. The dynamic deployment approaches in public cloud computing are security assessment, work flow deployment, policy assignment, audit data and policy analysis.

Qiang Guo et.al [8] gives the unique definition for trust in cloud computing and various issues related to trust are discussed here. An extensible trust evaluation model named ETEC has been proposed which includes a time-variant comprehensive evaluation method for expressing direct trust and a space variant evaluation property for calculating recommendation trust. An algorithm based on ETEC model is also shown here. This model also calculates the trust degree very effectively and reasonably in cloud computing environments.

***Bakshi et. al.* [9]** proposed another cloud intrusion detection solution. The main concern was to protect the cloud from DDoS attacks. The model uses an installed intrusion detection system on the virtual switch and when a DDoS attack is detected.

Xie [10] used Support Vector Machine (SVM) in spam detection. They found two optimal parameters, cost and gamma. They used a good method for selecting proper values of them, which is called "grid search", i.e. to search for the values of certain parameters over supplied parameter ranges. Although they performed parameters optimization, their detection rates were too low. They also did not perform feature selection

3. FUNDAMENTAL THEORY

3.1 Intrusion Detection System:

An Intrusion Detection System (IDS) constantly monitors actions in a certain environment and decides whether they are part of a possible hostile attack or a legitimate use of the environment. The environment may be a computer, several computers connected in a network or the network itself. The IDS analyzes various kinds of information about actions emanating from the environment and evaluates the probability that they are symptoms of intrusions. Such information includes, for example, configuration information about the current state of the system, audit information describing the events that occur in the system (e.g., event log in Windows XP), or network traffic. Several measures for evaluating The more widely used measures are the True Positive (TP) rate, that is, the percentage of intrusive actions (e.g., error related pages) detected by the system, False Positive (FP) rate which is the percentage of normal actions (e.g., pages viewed by normal users) the system incorrectly identifies as intrusive, and Accuracy which is the percentage of alarms found to represent abnormal behavior out of the total number of alarms. In the current research TP, FP and Accuracy measures were adopted to evaluate the performance of the new methodology.

3.2 Network Profiling:

Since the number of attacks is always increasing, IDS should be updated with signature for new attacks. Network profiling can help IDS to define labels of new signatures. There are some problems in network profiling such as grouping the attacks that come through the network based on their types. Those problems can be solved using data mining techniques such as clustering and classification [14, 15]

4. PROPOSED APPROACH

We propose a algorithms for network intrusion detection

Adaptive resonance theory (ART) is a theory developed by Stephen Grossberg and Gail Carpenter on aspects of how the brain processes information. It describes a number of neural network models which use supervised and unsupervised learning methods, and address problems such as pattern recognition and prediction. The primary intuition behind the ART model is that object identification and recognition generally occur as a result of the interaction of 'top-down' observer expectations with 'bottom-up' sensory information. The model postulates that 'top-down' expectations take the form of a memory template or prototype that is then compared with the actual features of an object as detected by the senses. This comparison gives rise to a measure of category belongingness. As long as this difference between sensation and expectation does not exceed a set threshold called the 'vigilance parameter', the sensed object will be considered a member of the expected class. The system thus offers a solution to the 'plasticity/stability' problem, i.e. the problem of acquiring new knowledge without disrupting existing knowledge.

ART1 model description:

ART1 is an unsupervised learning model specially designed for recognizing binary patterns. It typically consists of an attentional subsystem, an orienting subsystem as shown in Fig. 1, a vigilance parameter and a reset module. The vigilance parameter has considerable influence on the system. High vigilance produces higher detailed memories such as fine categories etc, while lower vigilance results in more general memories. The ART1 attentional has two competitive networks, comparison field layer F1 and the recognition field layer F2, two control gains, Gain1 and Gain2 and two short-term memory (STM) stages F1 and F2. Long-term memory (LTM) traces between F1 and F2 multi-ply the signal in these pathways

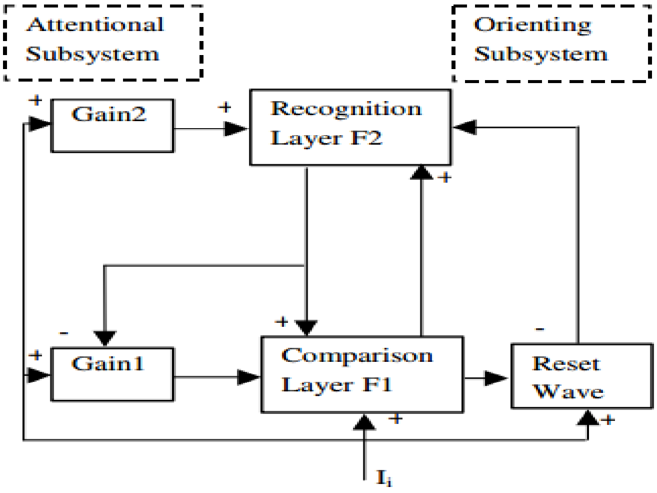

Fig. 1: Adaptive Resonance Theory Structure

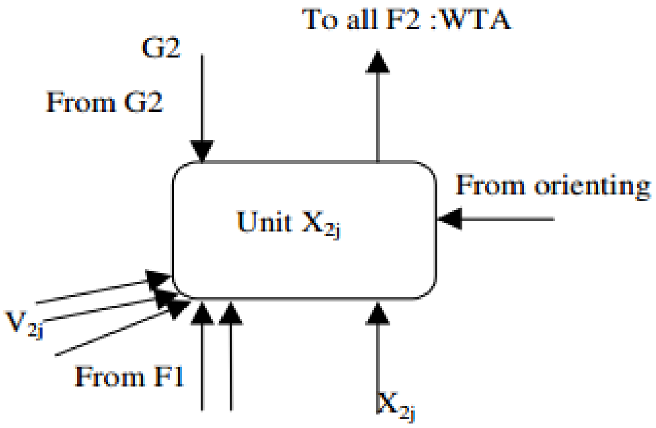

Fig. 2: Processing element X2jin layer F2

Gains control enables F1 and F2 to distinguish current stages of running cycle. STM reset wave inhibits active F2 cells when mismatches between bottom-up and top-down signal occur at F1. The comparison layer receives the binary external input passing it to the recognition layer responsible for matching it to a classification category. This result is passed back to the comparison layer to find out if the category matches that of the input vector. If there is a match a new input vector is read and the cycle start again. If there is a mismatch the orienting system is in charge of inhibiting the previous category in order to get a new category match in the recognition layer. The two gains control the activity of the recognition and the comparison layer respectively. The orienting subsystem generates a reset wave to F2 when the bottom-up input pattern and top-down template pattern at F1, according to the vigilance criterion. The reset wave selectively and enduringly inhibits active F2 cell until the current is shut off. Offset of the input pattern terminates its processing at F1 and triggers offset of Gain2. Gain2 offset causes rapid decay of STM at F2 and thereby prepares F2 to encode the next input pattern without bias. ART1 implementation: As state above, ART1 is a self organizing neural network having input and output neurons mutually coupled via bottom-up and top-down adaptive weights that perform recognition. To begin our approach, the network is first trained in accordance with the adaptive resonance theory by inputting reference pattern data under the form of 5×5 matrix (the very novelty of this study) into the neurons for clustering within the output neurons. Next, the maximum number of nodes in F2 is defined following by the vigilance parameter. The inputted pattern registered itself as short-term memory activity across a field of nodes F1. Converging and diverging pathways from F1 to a coding field F2, each weighted by an adaptive long-term memory trace, transform into a net signal vector T. Internal competitive dynamics at F2 further transform T, generating a compressed code or content addressable memory. With strong competition, activation is concentrated at the F2 node that receives the maximal F1→F2 signal. The main focus of this work is divided in four phases as follows: Comparison, recognition, search and learning.

The algorithm of ART-1 follows:

- Initialize the number of current templates
- Initialize set of templates
- Get a pattern from X
- Set flag “new node needed”
- Compute activation value for all templates
- Search for resonance
- Find template with highest activation value
- When resonance occurs
- Update the template

- No new node needed
- Stop the search for the resonant node
- If resonance doesn't occur,
- Reset wJ
- Continue search for resonant node
- Create new node if needed
- End of learning loop

5. EVALUATION MEASURES

To evaluate the system performance the following measures (based on Sequeira and Zaki 2002) were used.

True Positive Rate (TP) (also known as Detection Rate or Completeness): the percentage of terrorist pages receiving a rating above the threshold in the experiments, terrorist pages will be obtained from the users simulating terrorists.

False Positive Rate (FP): the percentage of regular Internet access pages that the system incorrectly determined as related to terrorist activities, i.e., the percentage of non-terrorist pages receiving a rating above threshold and suspected falsely as terrorists.

Accuracy: percentage of alarms related to terrorist behavior out of the total number of alarms. Since no benchmark data on content based intrusion detection is currently available, the results are compared to the best numbers achieved with ADMIT which is a command level method using the Means clustering algorithm to detect intruders.

6. CONCLUSION

An approach for a neural network based intrusion detection system, intended to classify the normal and attack patterns and the type of the attack, has been presented in this paper. We applied Improved ART-1 method which increased the generalization capability of the neural network and at the same time decreased the training time. It should be mentioned that the long training time of the neural network was mostly due to the huge number of training vectors of computation facilities. However, when the neural network parameters were determined by training, classification of a single record was done in a negligible time. Therefore, the neural network based IDS can operate as an *online* classifier for the attack types that it has been trained for. The only factor that makes the neural network off-line is the time used for gathering information necessary to compute the features. In this paper we introduce Improved ART-1 in a IDS to protect user. This algorithm is intended to be scalable by allowing different format of data to apply into ART-1 for more reliable IDS solution. The implemented ART-1 is just a first step in the direction of a complex CIDS. An interesting future topic is the implementation of the fully functional Improved ART-1 on the real internet tested. To practically apply the deployment, performance and scalability issues need to be considered as the next step.

REFERENCES

[1] Mahesh s,Mahesh T R, M Vinayababu (2010) " Using Data Mining Techniques for Detecting terror related activities on the web", Journal of Theoretical and Applied information technology

[2] Abbasi, A., & Chen, H. (2005). Applying authorship analysis to extremist group Web forum messages. IEEE Intelligent Systems, Special Issue on Artificial Intelligence for National and Homeland Security, 20(5), 67–75.

[3] Baumes, J., Goldberg, M., Hayvanovych, M., Magdon-Ismail, M., Wallace, W., & Zaki, M. (2006). Finding hidden group structure in a stream of communications. In S. Mehrotra, D.D. Zeng, & H. Chen (Eds.), Proceedings of the IEEE Conference on Intelligence and Security Informatics (pp. 201–212). Los Alamitos, CA: IEEE.

[4] Chen, H. (2006). Intelligence and security informatics: Information systems perspective. Decision Support Systems: Special Issue on Intelligence and Security Informatics, 41(3), 555–559.

[5] Chen, H., Qin, J., Reid, E., Chung, W., Zhou, Y., Xi, W., et al. (2004). The dark Web portal: Collecting and analyzing the presence of domestic and international terrorist groups on the Web. In W.T. Scherer & B.L. Smith (Eds.), Proceedings of the 7th IEEE International Conference on Intelligent Transportation Systems, (pp. 106–111).

[6] Brian Hay, Kara Nance, Matt Bishop, "Storm Clouds Rising: Security Challenges for IaaS Cloud Computing" Proceedings of the 44th Hawaii International Conference on System Sciences -2011. J.Allen, A. Christie, W.Fithen, j.McHugh,J.pickel, and E.Stoner, "State of the practice ofIntrusion Detection Technologies", CMU/SEI-99-TR-028, Carnegie Mellon Software Engg.Institute. 2000.

[7] John C.Mace, Aad van Moorsel, Paul Watson, "The Case for Dynamic Security Solutions in Public Cloud Workflow Deployments" School of Computing Science & Centre for Cybercrime and Computer Security (CCCS) Newcastle University, Newcastle upon Tyne, NE1 7RU, UK.

[8] Qiang Guo, Dawei Sun, Guiran Chang, Lina Sun, Xingwei Wang, "Modeling and Evaluation of Trust in Cloud Computing Environments" School of lnformation Science and Engineering, Northeastern University, Shenyang, P.R. China, Computing Center, Northeastern University, Shenyang, P.R. China, 2011 3rd International Conference on Advanced Computer Control (ICACC 2011).

[9] Bakshi, Chun-Chieh Huang, Joy Ku, "A Cooperative Intrusion Detection System Framework for Cloud Computing Networks", 39th International Conference on Parallel Processing Workshops, 2010.

[10] Y. Xie. An Introduction to Support Vector Machine and Implementation in R. May 2007.

[11] Wikipedia-Cluster Analysis, http://en.wikipedia.org/wiki/cluster_analysis.

[12] Johan Zeb Shah and anomie bt Salim, "Fuzzy clustering algorithms and their application to chemical datasets", in Proc. Of the post graduate Annual Research seminar 2005, pp.36-40.

[13] Zhengxim Chen, "Data Mining and Uncertain Reasoning-An integrated approach", Willey, 2001.

[14] Witcha Chimphlee, et.al. "Un-supervised

[15] Clustering methods for identifying Rare Eventsin Anomaly detection", in Proc. Of World Academy of Science, Engg. And Tech (PWASET), Vol.8, Oct2005, pp.253-258.

[16] J.Bezkek, "pattern Recognition with fuzzy objective function algorithms", Plennum Press,USA, 1981.

[17] S.Albayrak, and Fatih Amasyali, "Fuzzy CMeans clustering on medical diagnostic

[18] Systems", International XII Turkish Symposium on Artificial Intelligence and Neural Networks,TAINN-2003.