International Journal of Scientific Engineering and Technology Research

ISSN 2319-8885
Vol.04,Issue.08,
April-2015,
Pages:1477-1479

www.ijsetr.com

Enhanced Intrusion Detection System using Crisp Controller

VRUSHALI PATIL[1], YOGESH KATE[2], VIVEK BONDE[3], PUNAM PATIL[4]

[1]Dept of Computer Engineering, Shram Sadhana Trust College of Engineering, Jalgaon, India, E-mail: vrushalipatil1707@rediffmail.com.
[2]Dept of Computer Engineering, Shram Sadhana Trust College of Engineering, Jalgaon, India, E-mail: ykate49@gmail.com.
[3]Dept of Computer Engineering, Shram Sadhana Trust College of Engineering, Jalgaon, India, E-mail: vivekkbonde@gmail.com.
[4]Dept of Computer Engineering, Shram Sadhana Trust College of Engineering, Jalgaon, India.

Abstract: Security has become a crucial issue for computer systems due to the rapid expansion of computer networks. The detection of attacks against computer network is becoming a harder problem to solve in the field of Network security. Intrusion Detection System (IDS) is an essential mechanism to protect computer systems from many attacks. The major work of intrusion detection systems is used to detect the anomaly and new attackers in the networks. As the transmission of data over the internet increases the need to protect connected system also increases. Existing system present an anomaly-based intrusion detection system with the help of fuzzy controller. But to improve the system performance and accuracy, Crisp controller is used in proposed system given in this paper. Crisp controller is used to create a detection model in the training phase and update this model in the test phase.

Keywords: Intrusion Detection System (IDS), Crisp Controller.

I. INTRODUCTION

The Major work of intrusion detection systems is used to detect the anomaly and new attackers in the networks. The detection of attacks against computer networks is becoming a harder problem to solve in the field of Network security. Intrusion detection as defined by the Sys-Admin, Audit, Networking, and Security (SANS) Institute is the art of detecting inappropriate, inaccurate or anomalous activity. Today intrusion detection is one of the high priority and challenging tasks for network administrators and security professionals. More sophisticated security tools mean that the attackers come up with newer and more advanced penetration methods to defeat the installed security systems. Thus, there is a need to safeguard the networks from known vulnerabilities and at the same time take steps to detect new and unseen, but possible, system abuses by developing more reliable and efficient intrusion detection systems. Any intrusion detection system has some inherent requirements. Its prime purpose is to detect as many attacks as possible with minimum number of false alarms, i.e., the system must be accurate in detecting attacks. However, an accurate system that cannot handle large amount of network traffic and is slow in decision making will not fulfill the purpose of an intrusion detection system. We desire a system that detects most of the attacks, gives very few false alarms, cope with large amount of data, and is fast enough to make real-time decisions.

II. BACKGROUND

Intrusion detection started in around 1980s after the influential paper from Anderson. Intrusion detection systems are classified as network based, host based, or application based depending on their mode of deployment and data used for analysis. Additionally, intrusion detection systems can also be classified as signature based or anomaly based depending on the attack detection method. The signature-based systems are trained by extracting specific patterns (or signatures) from previously known attacks while the anomaly-based systems learn from the normal data collected when there is no anomalous activity. Another approach for detecting intrusions is to consider both the normal and the known anomalous patterns for training a system and then performing classification on the test data. Such a system incorporates the advantages of both the signature-based and the anomaly-based Systems and is known as the Hybrid System. Hybrid systems can be very efficient, subject to the classification method used, and can also be used to label unseen or new instances as they assign one of the known classes to every test instance. This is possible because during training the system learns features from all the classes. The only concern with the hybrid method is the availability of labeled data. However, data requirement is also a concern for the signature- and the anomaly-based systems as they require completely anomalous and attack free data, respectively, which are not easy to ensure. This intrusion detection system was used in MANET using Fuzzy controller.

III. EXISTING SYSTEM

Every system or computer in world is prone to attacks. Attackers can steal data, harm system, create nuisance in programs, creates noise. The attackers are called as Intruders. The current Intruder Detector System (IDS) operates on Fuzzy Logic or Fuzzy Control. Fuzzy Controller operates over a range of values from 0-1. It has provision to operate

over the decimal values too. It operates over fuzzy data. And KDD data set is used for operation.

IV. PROPOSED SYSTEM

Intrusion detection system using crisp controller and NSL data set for network based IDSs. NSL data set in which input of current network traffic is fed to the crisp controller. System checked the behavior of malicious attack and according to the training given to the system it removes the attacks. Due to use of Crisp controller, it only tracks the true behavior and hence performance of the system increases. Two main reasons for introducing crisp logic for intrusion detection are Intrusion detection involves many quantitative features. To categorize these quantitative features in order to establish high-level patterns, Crisp theory provides a reasonable and efficient way. And the Security itself is crisp. For quantitative features, there is no sharp delineation between normal operations and anomalies. Crisp episode rules allow one to create the high-level sequential patterns representing normal behavior. With crisp spaces, crisp logic allows an object to belong to different classes at the same time. This concept is helpful when the difference between classes is not well defined. This is the case in the intrusion detection task, where the differences between the normal and abnormal classes are not well defined. Thus the intrusion detection problem (IDP) is a two-class classification problem: the goal is to classify patterns of the system behavior in two categories (normal and abnormal), using patterns of known attacks, which belongs to the abnormal class, and patterns of normal behavior. In crisp logic, crisp sets define the linguistic notions, and membership functions define the truth-value of such linguistic expressions. Intrusion detection has been done in different phases which include training to the system, pre-processing and characterization of data sets, detecting intruders in the network with the status report for recognizing intruder in the network.

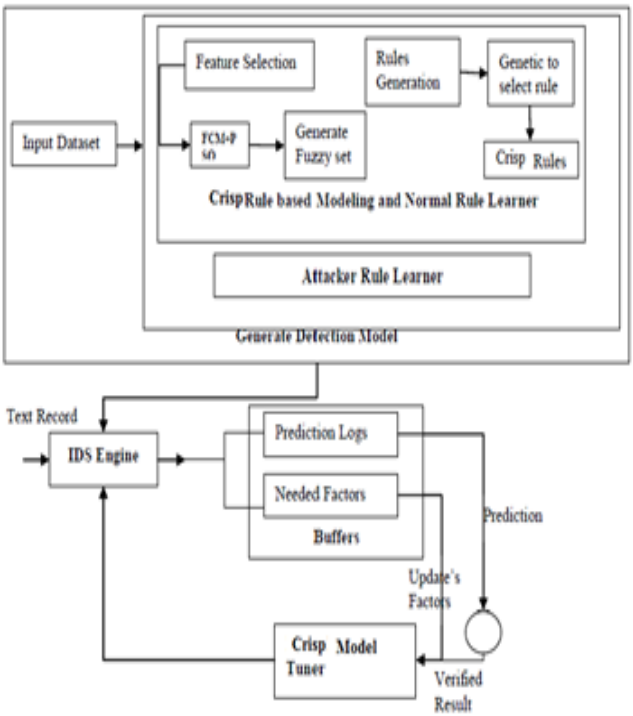

Fig.1. IDS using Crisp Controller.

A. Training Phase

IDSs are trained and data sets are categorized. The training will be provided to server as per data set, it's nothing but only feeding server with behavior to be checked. It is nothing but learning phase for the system. Temporary data set stores NSL data set which is multidimensional array with output results. NSL set consist of features of data with their output values which further use for the classification and testing of the records.

B. Testing Phase

Depending on the behavior of the system, intruder (anomaly) system or normal system is characterized. Then detection process starts with detection model generator which generates the framework for the detection process. The IDS engine employs the detection model to classify test samples. It monitors the work flow of the system as shown in Fig.1. Prediction logs and compatibility of test samples with each rule are buffered. Buffers maintain all the information about intruder and normal systems.

Given data sets are classified using Naïve Bayes algorithm. Naïve Bayes is probability based algorithm. The classified datasets gives standard mean and deviation values after testing phase. Where, mean is average of standard values of datasets and deviation is mean deviation of datasets. Crisp logic is applied on the probabilistic values generated by Bayesian classifier to get resultant value for that particular record is intruder or not. This procedure can be done in following steps-

Step 1: Calculate individual Probability of every feature.

Step 2: calculate probability by grouping the features.

Step 3: Calculate Final Probability of complete record finding values of Anomaly System and Normal System.

Step 4: Generate Output value from Maximum Probability value from step-3.

Step 5: Apply Crisp Logic on generated output value and get the Crisp value.

V. EXPERIMENTAL RESULTS

As mentioned above, due to changes in normal behaviour of the network and appearance of new attacks, using the static model for intrusion detection systems is not relevant. Here we have improved the performance of intrusion detection by updating the detection model substantially. This section describes the experimental result obtained for Proposed Crisp controller based Intrusion detection system. To compare the results with Crisp based IDS and Fuzzy Based IDS as Shown in Table 1.

TABLE I: Compare the Results with Crisp Based IDS and Fuzzy Based IDS

Systems	True Positive	True Negative	False Positive	False Negative	Accuracy
Crisp Controller	91	34	66	09	86
Fuzzy controller	86	42	58	14	79

VI. CONCLUSION

Anomaly based intrusion detection systems are provided in order to protect computer networks against novel attacks and improve network security. These systems perform intrusion detection by comparing current network traffic with a behavioural model of normal network activity. In this, we have addressed the dual problem of Accuracy and Efficiency for building robust and efficient intrusion detection systems. Our experimental results will show that Crisp Controller is very effective and accurate in improving the attack detection rate. To improve the accuracy for detect the anomaly in the intrusion detection system we extend our work with Genetic algorithm. Further improvements of intrusion detection systems can be done by applying standard clustering algorithms.

VII. ACKNOWLEDGEMENT

Authors of this paper would like to thank our College, SSBT's COET Bambhori, Jalgaon, NMU University, Maharashtra, India, for providing us adequate resources to make this paper. Also, we would like to thank our project guide Mr. S.D.Rajput and HOD Dr. G.K.Patnaik for their valuable suggestions.

VIII. REFERENCES

[1]K.Kavitha and S.Ranjitha Kumar, "Particle Swarm Optimization For Adaptive Anomaly-Based Intrusion Detection System Using Fuzzy Controller", International Journal of Computer Trends and Technology (IJCTT) Volume 4– Issue 10, Oct 2013.

[2]J.S.Narendra Kumar, T.Sudha Rani and M.Raja Babu, "Accuracy and Efficiency in Intrusion Detection System", IJCST, Volume-3, Issue 1, SPL 5, March 2012.

[3]Sandip Ashok Shivarkar and Mininath Raosaheb Bendre, "Hybrid Approach for Intrusion Detection Using Conditional Random Fields", International Journal of Computer Technology and Electronics Engineering (IJCTEE)Volume 1, Issue 3.

[4]Jonatan Gomez and Dipankar Dasgupta, "Evolving Fuzzy Classifiers for Intrusion Detection", Proceedings of the 2002 IEEE Workshop on Information Assurance United States Military Academy, West Point, NY June 2001.

[5]S. Saravanan and Dr. R M. Chandrasekaran, "Intrusion Detection System using Bayesian Approach", International Journal of Engineering and Innovative Technology (IJEIT) Volume 4, Issue 7, January 2015.

[6]Kamal Kishore Prasad and Samarjeet Borah, "Use of Genetic Algorithms in Intrusion Detection Systems: An Analysis", International Journal of Applied Research and Studies (IJARS) ISSN: 2278-9480 Volume 2, Issue 8 (Aug - 2013).