International Journal of Technology and Engineering System (IJTES)
Vol 7. No.3 2015 Pp. 213-218
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976-1345

A SURVEY OF INTRUSION DETECTION SYSTEM USING CLASSIFICATION

B.SENTHILNAYAKI[1], J.KAVYA[1] AND DR.K.VENKATALAKSHMI[2]
Department of Information Technology,UCEV1
Department of Electronics And Communication Engineering,UCET2
chandralekhamohandas@gmail.com

ABSTRACT

Due to the growing computer usage and network security of the computer system has become important. Every day new kind of attacks are being faced by industries. As the threat becomes a serious matter year by year, intrusion detection technologies are indispensable for network and computer security. Many techniques of Data Ming have been introduced to solve this problem. In this paper, a detailed survey of intrusion detection based on various techniques has been discussed. It is important to increase the detection rates and reduce false alarm rates in the area of intrusion detection. Here, the techniques are classified as Neural network, Support vector machine, K-means classifier and hybrid technique.

Keywords- Intrusion detection, Neural classifier, Support vector machine, K-means classifier, detection rate, false alarm rate

INTRODUCTION

The Vast application of computer networks, the quantity of attacks, hacking tools and intrusive methods have developed widely. One of the way of dealing with suspicious actions is by utilizing an intrusion detection system (IDS). By investigation of many records on the network [1] [2]. Intrusion detection detects computer attacks. To solve the network security problems it is one of the way. The important things to assess intrusion detection systems (IDS) Detection of attack signatures in the network [3]. Intrusion explained as an act of encroaching or infringing the reliability, confidentiality or avoiding the accessibility of a resource. And also to detect and tackle with the worm programs [4]. Intrusions Detection Systems discovers illegal or malicious. To perceptive files, these harasses can acquire quite a few forms like network attack against vulnerable services, data driven attacks on applications, host based attacks such as illegal logins and access. IDSs can be classified as misuse detectors and anomaly detectors by sorting out broadly based on their models of detection. The irregularity detection develops user profiles as the basis of detection, and sorts the distinctiveness of the unexpected from the normal ones as incursion [5, 6, 7,8 and 12]. Mishandling detectors rely on understanding the models of known attacks [5, 6 and 12].

It is becoming hard for intrusion detection system to suggest a repair with the varying technology. A new approach is used where the neural networks is used for the detecting the process of misuse. The Artificial neural networks increase the potential of the networks [9]. The Large growth of Internet traffic it has been created that a behavioral model exists in the attacks which can be known from former study. Various algorithms, such as Neural Network , Support Vector Machine, Genetic Algorithm, Fuzzy Logic and Data Mining etc.

SURVEY OF INTRUSION DETECTION

This section presents study of various intrusion detection classifier techniques. Many research papers regarding to intrusion detection are discussed and are widely classified into i) Neural network ii) Support vector machine iii) K-means classifier iv hybrid techniques and v)other detection techniques.

NEURAL NETWORK BASED INTRUSION DETECTION

A Many papers have been presented to represent the neural network based intrusion detection. Some of the papers have been discussed below. The neural network (NN) and decision tree (DT) for intrusion detection and the concept of anomaly detection and use both has been improved by M. Bahrololum et al. [13]. Decision Trees are very much efficient in discovering known attacks, The

Neural networks added advantage to it. They designed the system using together with DT and mixture of unsupervised and supervised NN for Intrusion Detection System (IDS). The Decision Trees gave a quick implementantion. The Neural network are based on hybrid of Self Organizing Map (SOM) and supervised NN based on Back propagation for complete grouping. M. Bahrololum et al. published a paper to deal with a hybrid of misuse and irregularity detection for training of normal and attack packets. Known packets were recognized fast by misuse approach and unknown attacks will be able to spot by this method. The method used for attack training was the mixture of unsupervised and supervised Neural Network for Intrusion Detection System. Attacks was categorized into smaller categories taking into consideration their similar features by the unsupervised NN based on Self Organizing Map (SOM), and followed by unsupervised NN based on Back propagation was utilized for grouping.

SUPPORT VECTOR MACHINE BASED INTRUSION DETECTION

The Review of Support Vector Machine classifier is discussed

Briefly here in this section. In the period 2007-2012, a lot of papers have represented the Support vector machine based intrusion detection. Many of the papers have been discussed below. The Genetic algorithm is used to select proper fields in the traffic packets and apply time delay using SVM [10]. Improvement of the training time of SVM has been presented by Latifur Khan et al. [14], with large data sets using hierarchical clustering analysis. Dynamically growing Self Organizing Tree is used for gathering, since it had many advantages over the disadvantages of traditional hierarchical clustering algorithms (e.g., hierarchical agglomerative clustering).

Among two classes, clustering analysis assisted discover the boundary points, which were the most capable data points to coach SVM. They offer an very good approach of amalgamation of SVM and DGSOT by the help of the clustering arrangement created by the DGSOT algorithm which in progress with a first training set and enlarge it slowly. In terms of precision loss and training time gain by means of a single bench-mark real data set they match up to their approach with the Rocchio Bundling technique and casual choice.To change the key in models into a feature space the Principal Component Analysis (PCA) was applied.

The Support Vector Machine (SVM) was employed for categorization reason. In addition, a proportional study was prepared with presented approaches [15]. Selecting of a suitable quantity of principal components was an important problem. As an alternative of using conventional method, Genetic Algorithm (GA) was applied in the optimum choice of principal components accordingly. The KDD-cup dataset was applied that was a benchmark for assessing the safety identification mechanisms. Therefore, the technique presented optimal interference detection mechanism was proficient to minimize amount of features and maximize the identification rates.

An intelligent multi level classification technique was proposed for effective intrusion detection in Mobile Ad-hoc Networks in the same year. The algorithm used a combination of a tree classifier which used a labeled training data and an Enhanced Multiclass SVM algorithm. Moreover, an effective preprocessing technique had been proposed and implemented in this work in order to improve the detection accuracy and to reduce the processing time. As a way of dealing with conditions for independent labeling of regular traffic where class distribution does not present the imbalance necessary for SVM algorithms, an approach has been presented by Carlos A. Catania et al. [16] in 2012. In such case, the self-governing labeling process was made by SNORT, a misuse-based intrusion detection system. The use of the planned autonomous labeling approach not only outperforms presented SVM alternatives that was shown by the experiments conducted on the DARPA dataset. It has more developments over SNORT itself .

K-MEANS ALGORITHM BASED INTRUSION DETECTION

In this section, we discuss the different papers about k-means algorithm. In 2003-2004 some papers presented to represent the K-means algorithm based intrusion detection. Some of the papers have been discussed below. In the year 2003, a K-means based clustering algorithm, named Y-means, for incursion detection has been offered by Yu Guan *et al.* [17]. Y-means surmounts two failings of K-means: quantity of clusters dependency and degeneracy A suitable number of clusters were divided routinely. This was one of the benefits of the Y-means algorithm for intrusion detection. The unprocessed log data of information systems can directly be applied as training data with-out being physically labeled was the another advantage.

To improve the learning capacities and decrease the computation strength of a competitive learning multi-layered neural network. Through a back propagation learning means the recommended model used multi-layered network structural design. The acquired results showed that the suggested technique executes specially in terms of both precision and computation time when pertained to the KDD99 dataset match up to a normal learning schema that utilized the full dataset. To decrease the amount of examples to be offered to the neural network, the K-means algorithm was initially used to the training dataset by automatically choosing a most favorable set of samples.

HYBRID TECHNIQUE BASED INTRUSION DETECTION

In the period 2007-2012, a lot of papers have been presented to represent the hybrid technique based intrusion detection. Some of the papers have been discussed below. Many quantitative feature involved in intrusion detection and security is Fuzzy. The integration of Association rules and fuzzy logic make the intrusion detection more flexible [11]. For categorizing irregular and normal activities in a computer network, a dynamic electronic circuit, and a motorized mass-beam system have offered a method to flow k-Means grouping and the ID3 decision tree learning. By means of Euclidean distance resemblance the k-Means grouping method first divided the training cases into k clusters. On every cluster, an ID3 decision tree on behalf of a density region of normal or anomaly instances has been constructed. By studying the subgroups inside the cluster the decision tree on every cluster purified the decision boundaries.

The conclusions of the k-Means and ID3 methods were united using two rules to get a concluding decision on classification. The two rules are: 1) the Nearest-neighbor rule and 2) the Nearest-consensus rule. Testing were executed by them on three data sets: 1) Network Anomaly Data (NAD), 2) Duffing Equation Data (DED), and 3) Mechanical System Data (MSD), which enclosed measurements from three separate application domains of computer networks, an electronic circuit applying a forced Duffing Equation, and a mechanical system, correspondingly. three techniques containing two machine-learning paradigms has been built up. K-Means Clustering, Fuzzy Logics and Neural Network techniques were arranged to get an efficient intrusion detection.

The huge rate of false alerts makes unnecessary human works which are manual and frequent in the traditional techniques of Intrusion Detection Systems. In order to solve these major problems in the traditional intrusion Detection Systems K-Means-Fuzzy-Neuro techniques are used. The technique was examined with the help of DARPA network traffic datasets. The results were excellent in reducing the false alarm rate and improving the capacity of the intrusion Packets.

The dimension of the feature sets are reduced by Deep belief network and is followed by the SVM to classify the intrusion. The intrusion is classified into five: Normal, R2L,Dos,U2R and probing [20]. The pattern matching approach for NIDS is based on the fusion of multiple classifiers [22]. To solve the problems and help the Intrusion Detection for higher detection rate, less false positive rate and stronger constancy based on ANN and Fuzzy clustering approach FC-ANN has been offered by Gang Wang et al. [25]. The process in FNN is: initial Fuzzy clustering system is used to produce dissimilar Data sets. Depending on the different training subsets dissimilar ANN models are put together consequently. At last, to summative those results a meta-learner, fuzzy aggregation module, were utilized. Investigational results on the KDD CUP 1999 dataset proved that their offered approach, FC-ANN.

Hybridization plan has been related and Detection imaging has been selected to see the capability and accuracy. To cut the dimensionality. To cut the dimensionality of the feature sets they employ of the feature sets they employed. Tests on NSL-KDD dataset were offered by them to assess the performance of their approach and demonstrated that the on the whole accuracy proposed by the utilized approach was high. It was pursued by a support vector machine to categorize the interference into five product; Normal, R2L, DoS, U2R, and Probing. The Data mining Algorithms like Naïve Baysian, Decision Tree, JRip, iBK are used here. They use four base classifiers and three ensemble algorithms. But it is unsuccessful. Because it has less accuracy rate in the Intrusion Detection. This method improved the performance of the model. The Supervised or unsupervised data filtering with the classifiers of cluster first o the whole training data sets is followed and the output is given to the other classifers. The proposed method has detection rate and low false alert rate. It was proved by experiments on NSL-KDD datasets ie., an improved version of KDD cup 1999 dataset.

OTHER CLASSIFIER BASED INTRUSION DETECTION

Here, we discuss about the different papers of various intrusion detection techniques. In the year 2003-2012 a lot of papers have been presented to represent the classifier based intrusion detection. Some of the papers have been discussed below. A new approach to reduce false positives for intrusion detection using improved self adaptive Bayesian algorithm (ISABA) [19]. Qiuming A. Zhu et al presented the multi level hierarchy Kohonen Net (K-Map) [23] for network intrusion detection systems. Every level of the map was straight forward. The effectiveness is one of its major advantage.The Statistical Anomaly detection methods are extensively used. The Reduced network is one of its positivity. The Categorisation of K-Map was used for detecting anomalies. Subsets are selected that has both the attacks and normal records from KDD cup 1999 benchmark was used to hierarchial net. The testing and presentation assessment of the suggested model was performed by means of artificial network traffic, intimately on behalf of real-world DDoS attacks and FE traffic, a produced using a software-based traffic generator developed. Prasanta Gogoi et al. [24] have suggested an actual dataset to modernize this critical inadequacy. A test bed has been set up by them to begin network traffic of both attack as well as standard nature by means of attack tools. The evolution of the soft computing for Intrusion Detection System and was effectively explained in ints utility of training subset of KDD cup 99 dataset. For Interference detection, ANFIS was used as Neuro fuzzy classifiers. The human work is not necessary to find the number of rules and membership functions the enhanced classification subtractive clustering has used. To create the system more protective to the attacks using the fuzzy interference approach. So that the fuzzy engine was found. Fuzzy sets and the fuzzy logic are used for the efficient classification of the data [21]. Atlast, they used the genetic algorithms are used to optimize the fuzzy decision making algorithms. The Research was very successful.

COMPREHENSIVE ANALYSIS AND DISCUSSIONS

This section presents a comprehensive analysis of various methods such as neural network based, support vector machine based, k-means based, hybrid technique based and other techniques for intrusion detection. As we have discussed Classification is done based on intrusion detection with respect to the detection rate, time and false alarm rate achieved by the different methods.

NEURAL NETWORK BASED INTRUSION DETECTION

Table: 1 shows the comparison of intrusion detection using neural network technique. From the table, we can find that M. Bahrololum et al. [13] achieved detection rate of 93.8%.

Table 1: Comparison of intrusion detection using neural network

S. No	**Authors**	**Method/Algorithms**	**Detection rate (%)**	**False alarm rate**
1	M. Bahrololum *et al.* [13]	Neural network based on Hybrid Self Organizing Map (SOM)	91.3 %	-
2	M. Bahrololum *et al.* [13]	Neural network based on K Self Organizing Map (K- SOM)	93.8 %	-

SUPPORT VECTOR MACHINE BASED INTRUSION DETECTION

Table: 2 shows the comparison of some intrusion detection using support vector machine technique. From the table, it is found that Ahmad *et al.* [18] achieved a better detection rate 96.6% and false alarm 0.4% compared to others.

Table 2: Comparison of intrusion detection using support vector machine

S.No	Authors	Method/Algorithms	Detection rate (%)	False alarm rate
1	Carlos A. Catania *et al.* [16]	Support vector machine	87.02 %	-
2	Ahmad *et al.* [18]	Support vector Machine and neural networks	96.6%	0.4%

K-MEANS BASED INTRUSION DETECTION

Table: 3 shows the comparison of some intrusion detection using support vector machine technique. Yu Guan et al. [17] technique [89.9%]. On the other hand, false alarm rate is found to be 6.21%

HYBRID TECHNIQUE BASED INTRUSION DETECTION

Table: 3 shows the comparison of intrusion detection using two different techniques. From the table, it can be found that Iwan Syarif et al. [27] achieved a better detection rate values compared to others. In Mrutyunjaya Panda et al. [28] the detection rate is found to be 99.5% and the false alarm rate is found to be 0.1 which is lower when compared to other techniques. Technique Shekhar R. Gaddam et al. [23] achieved a better false alarm rate values compared to others and the detection rate is found to be 96.24%. In Gang Wang
detection using support vector machine technique. From the

Table 3: Comparison of intrusion detection using hybrid

techniques

S. No	Authors	Method/ Algorithms	Detection rate (%) (Accuracy)	False alarm rate (%)
1	Mrutyunjaya Panda *et al.* [26]	Decision trees, principal component analysis, SPegasos (Stochastic variant of Piramol estimated sub-gradient solver in SVM)	99.5%	0.1%
2	Gang Wang *et al.* [25]	Fuzzy C-means-Artificial Neural Network	96.71%	-

CONCLUSION

The Network Intrusion Detection System is the latest technology which is an important technology of the Network Security Nowadays there are many advanced technology for the Intrusion Detection Systems. Many classification techniques like Bayesian Classifiers, Neural networks, Support vector machine, Decision trees and K-Means etc are used. In this Survey we have clearly discussed about the Intrusion Detection

REFERENCE

1. Anderson, J.P," Computer Security Threat Monitoring And Surveillance," Technical Report, Vol.3, pp.234-267,1980.

2 Yang Li, Li Guo, "An Active Learning Based TCM-KNN Algorithm for Supervised Network Intrusion Detection ," Computers & Security, vol.26, pp.459-467, 2007.

3. Silva, L.D.S, Santos, A.C.Mancilha, "Detecting Attack Signature In The Real Network Traffic with ANNIDA", Expert Systems with Application, Vol.34, no.4, pp.2326-2333, 2008

4. Heady R., Luger G., Maccabe A.,And Survile M. "The Architecture Of Network Level Intrusion Detection System"
Technical Report Vol.6, pp.2365-2444,2010

5. Dennig D." Intrusion Detection Model", IEEE Transaction On Software Engineering, Vol.SE-B,No.2, pp.222-232,1989.

6. Kumar S., Spaffor E.H. "An Application Of Pattern Matching In Intrusion Detection ", Technical Report CSD-TR-94-013. Purde University, 1994.Vol.7, pp.256-266, 2007.

7. Ryan J.,Lin M.,"Intrusion Detection With Neural Networks",Advance In Neural Information Processing Systems,Vol.10,pp.289-298,2000.

8. Terran Lane, Carl E.Brodley," Temporal Sequence Learning And Data Detection For Anamoly detection " Vol.2,no.3,pp.229-331 aug-1999.

9. Cannady J." Artificial Neural Networks For Misuse Detection ",National Information System Security Conference,Vol.8,pp.226-2238,2001.

10. Shon T., J,"SVM Approach with A Genetic Algorithm for Network Intrusion Detection ",International symposium On Computer And Information Science Vol.9,pp.224-223,2005.

11. J.Luo And S.M.Bridges,"Minning Fuzzy Association Rules And Fuzzy Frequency For Intrusion Detection ",International
Journal Of Intelligent System.Vol.5,pp.687-703,2000.

12. W.K.Lee And S.J.Stolfo,"A Data Mining Framework For
Building Intrusion Detection Model ",IEEE Symposium on
Security And Privacy,Oaklan.Vol.4.pp.228-239,1999.

13. M. Bahrololum, E. Salahi and M. Khaleghi, "Anomaly intrusion detection design Using Hybrid of Unsupervised and supervised neural Network," International Journal of Computer Networks and Communication Vol.1, pp.234-
243, July 2009.

14. Latifur Khan, Mamoun Awad, Bhavani Thuraisingham,"A new intrusion detection system using SVM And Hierarchial
Clustering", Journal of VLDB Journal, Vol.16, pp.507-521, 2007.

15. Iftikhar Ahamed, Tzeen Abdullah, "Optimised Intrusion Detection System Using Soft Computing Techniques", Telecommunication System, Vol.34,2011.

16. Carlos A.Catania,"An Autonomous Labelling Approach to Support Vector Machine Algorithm for Network Traffic Anomaly Detectio.n", Expert System with Application Vol.39, pp.665-676,2012.

17. Yu Guan, Nakil Belachel and Ali A.Ghorbani, " Y-means: A Clustering Method For Intrusion Detection System", Conference on Electrical and Computer Engineering Vol.2,pp.233-243,2003.

18. Iftikhar Ahmad,Azween Abdullah,Abdullah Alghamdi,Muhammad Hussain,"Optimized intrusion detection mechanism using soft computing techniques," Telecommun System,2011.

19. Dewan Md. Farid, Mohammad Zahidur Rahman, "Anomaly Network Intrusion Detection Based on Improved Self Adaptive Bayesian Algorithm," Journal of Computers, Vol. 5, No. 1, January 2010.

20. Mostafa A. Salama, Heba F. Eid, Rabie A. Ramadan, Ashraf Darwish, and Aboul Ella Hassanien,"Hybrid Intelligent Intrusion Detection Scheme," Soft Computing in Industrial Applications Advances in Intelligent and Soft Computing,Vol.96, pp.293-303,2011.

21. Pavel Kromer, Jan Platos, Vaclav Snasel, Ajith Abraham," Fuzzy Classification by Evolutionary Algorithms," IEEE International Conference on Systems, Man, and Cybernetics (SMC),Vol.7, pp.313 - 318, 2011.

22. Giorgio Giacinto, Fabio Roli, and Luca Didaci, "Fusion of Multiple Classifiers for Intrusion Detection in Computer Networks," Journal of Pattern Recognition Letters, Vol.24, pp.1795-1803, 2003.

23. Qiuming A. Zhu, and Julie Huff "Hierarchical Kohonenen Net for Anomaly Detection in Network Security," IEEE Transactions on Systems, Man, And Cybernetics-Part B: Cybernetics, Vol. 35, No. 2, April 2005.

24. Prasanta Gogoi, Monowar H Bhuyan, D K Bhattacharyya, and J K Kalita,"Packet and Flow Based Network Intrusion Dataset," Contemporary Computing Communications in Computer and Information Science, Vol.306, pp.322-334, 2012.

25. Gang Wang, Jinxing Hao, Jian Ma, Lihua Huang, "A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering, " Expert Systems with Applications, Vol.8,pp.226-2238,2010.

26. Mrutyunjaya Panda, Ajith Abraham, Manas Ranjan Patra.a "A Hybrid Intelligent Approach for Network IntrusionDetection," International Conference onCommunication Technology and System Design, Procedia Engineering, vol. 30, pp.1-9,2012.