International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 4, April - 2014

# Survey on Intrusion Detection Techniques Using Data-Mining Domain

Uday Babu P.[1] Priya C. G[2] Visakh R.[3]
Department Of Computer Science & Engineering
Rajagiri School of Engineering & Technology
Cochin, India

***Abstract*—Intrusion is an illegal act of accessing or monitoring a system without proper authorization. Intrusion detection is of prime importance as intrusion can have catastrophic effect on the security of the victim system. Probe attacks, Denial of service attacks, Remote to local attacks and User to root attacks are the four main types of intrusions. KDD CUP 1999 is the fundamental data set widely exploited for evaluating the performance of intrusion detection methods.**

***Keywords— Intrusion Detection; Data Mining; NSL KDD; ISCX.***

## I. INTRODUCTION

In the current scenario where the attacks on the computer networks are escalating at a fast pace, intrusion detection is inevitable to safeguard the information systems. Intrusion detection is basically a two-class classification predicament which is capable of distinguishing between intrusions and normal connections [2].

### *A. Four main classes of intrusions*

There are predominantly four classes of intrusions namely DOS, Probe, R2L and U2R attacks [2].

- A denial of service attack (DOS) is any type of attack on a network to debilitate the server from providing services to its clients and there by revoking the ability of accessing a system from its authorized users. In Denial of Service attacks, the attacker makes some network so much occupied and busy that it will not be able to handle legitimate requests.
- Probe attack is a type of attack in which the intruder scans a network to harvest data for detecting vulnerabilities that may be exploited in the future.
- Remote-to-Local (R2L) attack is an attack in which the intruder forwards packets to a system over a network to exploit system's weakness to attain local access as a user. As a result, the intruder secures the privileges that a local user would have on the computer. Thus the vulnerabilities of the system get exposed.
- User-to-Root (U2R) attack is an attack in which an intruder, with access to a normal user account on the system, gains root access to the system. In short, the intruder would be exploiting his access to the system as a normal user in order to gain super user privileges.

Upcoming sections of this paper are constructed as follows: The benchmark datasets used for evaluating the performance of intrusion detection systems is being showcased in section II. Section III explains the basic methodology for intrusion detection. In section IV, an insight into various techniques prevailing for intrusion detection is presented. Followed by section V that elaborates on the measures available to figure out the efficiency of a given technique. Section VI concludes the survey.

## II. DATA SETS

KDD CUP 1999 is the standard de facto data set that is extensively used in evaluating intrusion detection techniques [7]. It incorporates 41 features which are classified into three classes. This database accommodates records attacks that assembled into four classes of intrusions and one class of normal connections [2]. KDD CUP data set has been strongly criticized for its shortcomings [6]. KDD CUP data set contains redundant records in the training set that misleads the classifiers. The presence of duplicate records in the testing set misdirects the learning algorithms. Duplicate records prevent the learning algorithms from learning about infrequent records. KDD CUP'99 data set is not an ideal representative of the prevailing real networks but due to lack of availability of real time and public data sets for intrusion detection systems, it is applied as a benchmark data set to assist the researchers working on intrusion detection systems.

In [6], NSL-KDD data set has been proposed which comprises of selected records of the KDD CUP'99 data set. NSL-KDD data set overcomes several limitations of the KDD CUP data set. It does not incorporate redundant records in the training set as a result the classifiers will not become biased towards the frequent records. It does not encapsulate duplicate records in the testing sets so the performance of the learners will not get biased by the methodologies which exhibit improved detection rates for frequent records. The cardinality of the records corresponding to each difficulty level group is inversely proportional to the percentage of records in the original KDD CUP'99 data set. As a result, the classification rates of different machine learning methods vary in a wider range and this makes NSL KDD data set to perform a precise assessment of distinct learning techniques.

NSL KDD data set embodies reasonable number of records in both training and testing sets. Hence the experiments can be

executed on the complete data set rather than randomly selecting a portion of the dataset which leads to comparable and consistent results. Even though NSL KDD CUP data set overcomes several shortcomings of KDD CUP'99 data set, still it cannot be considered as a ultimate representative of real networks due to presence of few shortfalls as mentioned in [8]. Compared to KDD CUP'99 data set, NSL KDD can be preferred to analyse the effectiveness of intrusion detection System in the absence of real time data sets [9].

Static datasets like KDD Cup'99, NSL KDD are immutable, outdated and they cannot be scaled. So a data set that represents realistic network traffic is vital to deal with network patterns and intrusions that are constantly evolving. ISCX 2012 is a dynamic, alterable, scalable, reproducible and labeled data set that captures network interactions completely and incorporates distinct intrusion scenarios to characterize the evolving intrusion patterns [10]. It includes network activities for a period of 7 days.

ISCX 2012 data set is constructed on the basis of profiles. Profiles comprises of extended descriptions of intrusions and abstract representative models for applications or protocols. Profiles can be exploited to generate real traffic. In short, ISCX 2012 data set can be considered as a true representative of real network traffic.

## III. BASIC METHODOLOGY

Basic methodology of majority of the intrusion detection techniques consists of three or four phases. Firstly, an apt data set must be selected for experimentation. Secondly, pre-processing is done on the selected data set. Thirdly, Feature extraction is done for dimensionality reduction by selecting the most productive records from the data set. Feature extraction is followed by an optional feature selection, where optimal subsets of features are selected. Performance of the classifier can be enhanced by performing feature selection and feature extraction. Third and fourth phases can be executed in any order with respect to each other. Fifth phase includes training and testing of the classifier that classifies the given connection either as normal or intrusive connection

## IV. INTRUSION DETECTION METHODOLOGIES

Majority of the techniques available for intrusion detection deals with extracting prime features from the KDD CUP'99 data set. These extracted optimal and minimal features are used to train a classifier to predict whether a connection is an intrusion or not. Each attack has its own unique patterns that need to be determined and these patterns may be evolving with time [15]. Data mining can be effectively applied to the domain of security.

In [1], an intrusion detection system based on SVM has been introduced, which merges BIRCH hierarchical clustering algorithm, a feature selection procedure and the classifier SVM. The hierarchical clustering algorithm was used to supply lesser and most significant training instances from the KDD Cup 1999 training set to SVM. Thus, the BIRCH hierarchical clustering algorithm was applied to discard inconsequential features from the training set and to get a reduced data set with high quality data points, so that SVM could classify the network traffic data more accurately with a short training period. In short, five different CF trees were constructed after transforming non-continuous attributes to continuous attributes and scaling. Four CF trees corresponding to each of the four types of attacks and one CF tree corresponding to normal connections are created. Feature selection was executed for each type of attacks. Four SVM classifiers corresponding to the four types of attacks was trained. The four SVMs classifiers are integrated to construct the intrusion detection system.

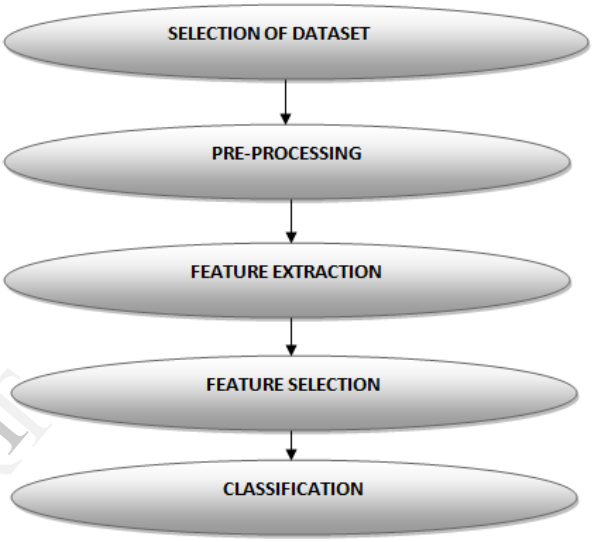


Fig. 1. Basic methodology for intrusion detection

There are 4 main types of intrusions, so an initial clustering on the data set is done using methods like k means clustering to create 4+1 clusters, 4 based on the type of intrusion and the additional 1 cluster represents the normal instances which are not intrusions [3]. Each cluster is then used to train a unique ANFIS based fuzzy neural network to extract one prime attribute from each cluster. The 5 attributes along with a membership function attribute is used to create 6 dimensional vectors to train SVM which performs the classification.

In [5], As a part of pre-processing, a subset of the KDD CUP 1999 data set is to be selected which incorporates due representation of all types of intrusion. This subset can be called representative instances. The representative instances can be spotted by initially partitioning the data set into subsets based on the class of the intrusions. Relevant number of instances in each class that effectively represents its class by being similar to k instances of its own class than being similar to the k instances of other classes can be considered as representative instances which are finally integrated to get an efficiently exploitable fold of the data set. This step can reduce the time and space complexity to a great extend. Similarity between two instances can be measured using Euclidean or Manhattan distances.

In [11], initially KDD CUP'99 data set is chosen for experimentation. Then feature transformation is performed by executing PCA to render the features in an organized and discriminated style in the principal space. PCA helps to deal with redundancy and to extract the principal components. GA is applied to explore the PCA space to pick a subset of principal components. Finally classification is done by using SVM, a two class classifier that can classify instances into two classes; intrusive and normal. Training and testing of the system is done to generate results.

In [12], Feature selection is carried out by applying PCA. 22 features where extracted from the KDD CUP'99 data set. The principal components corresponding to highest Eigen values are selected. At the last phase, classification is conducted by employing neural networks.

In [13], a hybrid intrusion detection system that integrates misuse detection and anomaly detection has been proposed. In misuse detection, random forests classification algorithm is used to create intrusion patterns from KDD CUP'99 data set and then network intrusions are detected by matching network connections to these intrusion patterns. The output of misuse detection phase is fed as the input of anomaly detection phase where weighted k-means clustering algorithm detects intrusions by clustering the data of network connections to gather the majority of the intrusions together in one or more clusters and the intrusive clusters are identified by inserting and comparing known attacks with unresolved connection's data. Misuse detection comprises of two phases. The initial offline phase constructs normal and intrusion patterns by processing the training dataset, followed by the online phase that detects intrusions depending on the patterns developed during the initial phase.

In [14], an intrusion detection technique that can detect unknown attacks on a network by recognizing the prime features of attack has been described. Initially, Data is collected for analysis by simulating real network traffic by running script for attacks. As a first phase, unsupervised k-means clustering is performed to create normal and intrusive (abnormal) clusters. During this phase, the relevant and effective features of each attack are extracted by processing abnormal clusters. The second phase performs feature selection by utilizing Naive Bayes classifier to determine and assign ranks to the relevant subset of features corresponding to each attack. Here Kruskal–Wallis test was engaged to extract statistically important features which were given rank accordingly. Final phase was classification using decision trees that discover rules and relationships by systematically dividing information contained within data. The collections of paramount features determined during the previous phase were classified with C4.5 decision tree algorithm that employs divide and conquer technique.

A novel approach for intrusion detection based on fuzzy logic and genetic algorithm has been proposed in [16]. A real time data set is utilized. The optimal set of features was determined using Genetic algorithm. These features will be used to train the set of rules. Fitness function was evaluated based on the accuracy and the number of attributes involved. Trapezoidal fuzzy sets are defined based on an initial set of parameters that are determined by the genetic algorithm. Parameters are encoded using three bit binary encoding. The gene for each feature in the chromosome requires 12 bits. These parameters are used to redefine and optimize the fuzzy rule set.

An intrusion detection system with hybrid neural networks namely RBF and Elman networks in the background has been proposed in [17] for anomaly and misuse detection. RBF network is responsible for performing classification in real time and Elman network attains the memory ability for supporting the RBF network's task. The hybrid model for intrusion detection is evaluated with DARPA data set. The adaptable system with memory ability has an easily configurable sensitivity and shows user defined tolerance to which neural network is transparent to. The proposed system succeeded in incrementing the detection rate.

Application Distributed Denial of Service (App-DDoS) is exploited by hackers or intruders to destroy the bandwidth of the target so as to reduce the number of services that will be granted to legitimate users per unit time. Vulnerabilities in the application-layer are utilized to accomplish this purpose and the complexity in tracking this attack is raised. In [18], a methodology is suggested to detect App-DDoS attacks by capturing browsing behaviours of users and network traffic which is represented in a sequence order independent style. A behaviours matrix is then constructed on which Principal Component analysis (PCA) is executed to reduce the dimensionality and to model the browsing behaviour. K means clustering is executed on the modelled behaviour to create k clusters. A threshold is computed using each cluster which is used to differentiate between normal and abnormal connections. Thus access to a system is allowed based on the threshold.

## V. EVALUATION OF INTRUSION DETECTION METHOLOGIES

Intrusion detection is the art of detecting inappropriate and anomalous activities by monitoring and analyzing the events occurring in computer systems. The performance of various intrusion detection methodologies can be quantified using the metrics like accuracy (ACC), detection rate (DR) (or sensitivity or true positive rate), false positive rate (FPR), Specificity (SPEC) (or true negative rate) and precision (PR) [15]. ACC, DR, SPEC and PR should be more close to one for an efficient intrusion detection methodology. FPR should be zero or more close to zero for a good intrusion detection methodology.

Sensitivity is the conditional probability that the methodology classifies an activity as an intrusion provided that activity was an intrusion. Specificity is the conditional probability that activity is an intrusion provided that the methodology classifies the activity as an intrusion. Accuracy represents the overall potential of the methodology. False positive rate portrays the rate at which false alarms are generated by the methodology. Precision states the degree at which the methodology produces correct alarms against intrusions.

True Positives (TP) are intrusion attacks accurately identified as intrusions by the methodology. True Negatives (TN) are the normal connections correctly identified as normal connections. False Positives (FP) are the normal connections which are incorrectly identified as intrusions. False Negatives (FN) are the intrusion attacks which are wrongly identified as normal connections.

Confusion matrix can be used to represent the performance of the methodology. It encapsulates the results of testing phase of the methodology. The performance of the methodology can be thus quantified using the confusion matrix. It captures the correct and incorrect classifications done by the classifier. Confusion matrix is shown in Table 1.

$$ACC = \frac{TP + FP}{TP + FP + TN + FN} \quad (1)$$

$$DR = \frac{TP}{TP + FN} \quad (2)$$

$$PR = \frac{TP}{TP + FP} \quad (3)$$

$$FPR = \frac{FP}{FP + TN} \quad (4)$$

$$SPEC = \frac{TN}{TN + FP} \quad (5)$$

TABLE I. CONFUSION MATRIX

| *Class* | *Intrusion (Prediction)* | *Normal (Prediction)* |
|---|---|---|
| ***Intrusion (Actual)*** | TP | FN |
| ***Normal (Actual)*** | FP | TN |

## VI. CONCLUSION

Intrusion detection is an inevitable component in the security services of any system. Timely detection of intrusions can prevent devastative effects by executing appropriate actions. Hence, intrusion detection safeguards integrity, confidentiality, availability and reliability of the system. A methodology with self evolving nature is yet to come to detect the mutating intrusion patterns. Detection of intrusions should be accompanied by necessary counter measures which should be well designed.

## REFERENCES

[1] Shi-Jinn Horng, Ming-Yang Su, Yuan-Hsin Chen, Tzong-Wann Kao, Rong-Jian Chen, Jui-Lin Lai, Citra Dwi Perkasa, "A novel intrusion detection system based on hierarchical clustering and support vector machines," Expert Systems with Applications, vol.38, Issue 1, Jan. 2011, pp. 306-313, ISSN 0957-4174, doi:10.1016/j.eswa.2010.06.066.

[2] V. Bolon-Canedo, N. Sanchez-Marono and A. Alonso-Betanzos, "Feature selection and classification in multiple class datasets: An application to KDD Cup 99 dataset," Expert Systems with Applications, vol.38, Issue 5, May 2011, pp. 5947-5957, ISSN 0957-4174, doi:10.1016/j.eswa.2010.11.028.

[3] A.M.Chandrasekhar and K.Raghuveer, "Intrusion Detection Technique using k-means, fuzzy neural networks and SVM Classifiers," International Conference On Computer Communication and Informatics 2013 (ICCCI 2013), Jan. 2013, vol.1, no.7, pp. 4-6, doi: 10.1109/ICCCI.2013.6466310

[4] P. Jongsuebsuk, N. Wattanapongsakorn and C. Charnsripinyo, "Network Intrusion Detection with Fuzzy Genetic Algorithm for Unknown Attacks," International Conference on Information Networking (ICOIN), Jan. 2013. vol.1, no. 5, pp. 28-30, doi: 10.1109/ICOIN.2013.6496342.

[5] Chun Guo, Ya-Jian Zhou, Yuan Ping, Shou-Shan Luo, Yu-Ping Lai, Zhong-Kun Zhang, Efficient intrusion detection using representative instances, Computers & Security, vol.39, Part B, November 2013, pp. 255-267, ISSN 0167-4048, doi:10.1016/j.cose.2013.08.003.

[6] Mahbod Tavallaee, Ebrahim Bagheri, Wei Lu and Ali A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," Computational Intelligence for Security and Defense Applications, 2009(CISDA 2009). IEEE Symposium on , vol., no., pp.1,6, 8-10 July 2009, doi: 10.1109/CISDA.2009.5356528

[7] Jaeik Cho, Changhoon Lee, Sanghyun Cho, Jung Hwan Song, Jongin Lim and Jongsub Moon, "A statistical model for network data analysis: KDD CUP 99' data evaluation and its comparing with MIT Lincoln Laboratory network data," Simulation Modelling Practice and Theory, vol.18, Issue 4, Apr. 2010, pp. 431-435, ISSN 1569-190X, doi:10.1016/j.simpat.2009.09.003.

[8] J. McHugh, "Testing intrusion detection systems: a critique of the 1998 and 1999 darpa intrusion detection system evaluations as performed by lincoln laboratory," ACM Transactions on Information and System Security, vol.3, no. 4, pp. 262–294, 2000.

[9] Nsl-kdd data set for network-based intrusion detection systems [Online]. Available: http://nsl.cs.unb.ca/NSL-KDD/, March 2009.

[10] Ali Shiravi, Hadi Shiravi, Mahbod Tavallaee and Ali A. Ghorbani, "Toward developing a systematic approach to generate benchmark datasets for intrusion detection," Computers & Security, vol.31, Issue 3, May 2012, pp. 357-374, ISSN 0167-4048, doi:10.1016/j.cose.2011.12.012.

[11] Iftikhar Ahmad, Muhammad Hussain, Abdullah Alghamdi and Abdulhameed Alelaiwi, "Enhancing SVM performance in intrusion detection using optimal feature subset selection based on genetic principal components," Neural Computing and Applications, Apr. 2013, pp. 1-12, ISSN 0941-0643, Springer-Verlag London.

[12] Guisong Liu, Zhang Yi and Shangming Yang, "A hierarchical intrusion detection model based on the PCA neural networks," Neurocomputing, vol.70, Issues 7–9, Mar. 2007, pp. 1561-1568, ISSN 0925-2312, doi:10.1016/j.neucom.2006.10.146.

[13] Reda M. Elbasiony, Elsayed A. Sallam, Tarek E. Eltobely and Mahmoud M. Fahmy, "A hybrid network intrusion detection framework based on random forests and weighted k-means," Ain Shams Engineering Journal, vol.4, Issue 4, Dec. 2013, pp. 753-762, ISSN 2090-4479, doi:10.1016/j.asej.2013.01.003.

[14] Panos Louvieris, Natalie Clewley and Xiaohui Liu, " Effects-based feature identification for network intrusion detection," Neurocomputing, vol.121, Dec. 2013, pp. 265-273, ISSN 0925-2312, doi:10.1016/j.neucom.2013.04.038.

[15] Uday Babu P and Visakh R. "A Proposed Methodology for Virus Detection Using Data Mining and Reverse Engineering Tools with Client-Server Model". International Journal of Computer Trends and Technology (IJCTT) V8(4):200-203, Feb. 2014. ISSN:2231-2803, doi:10.14445/22312803/IJCTT-V8P136.

[16] Terrence P. and Fries, "A fuzzy-genetic approach to network intrusion detection," In Proceedings of the 10th annual conference companion on Genetic and evolutionary computation (GECCO '08), Maarten Keijzer (Ed.). ACM, New York, NY, USA, Jul. 2008, pp. 2141-2146. doi:10.1145/1388969.1389037.

[17] Jianhua Wang and Yan Yu, "Research on Hybrid Neural Network in Intrusion Detection System," World Academy of Science, Engineering and Technology, International Science Index 76, 2013, vol.7(4), pp. 469-473.

[18] R. Bharathi and R. SukaneshA, "PCA Based Framework For Detection Of Application Layer DDoS Attacks," WSEAS Transactions On Information Science And Applications E-ISSN: 2224-3402, Dec. 2012, Vol.9, Issue 12.