Volume 4, Issue 1, January 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Q-learning Technique and Feature Extraction Methods Based Network Intrusion Detection for Real-time Systems

Sheikh Kashif Ahmed, Prof. Sriram Yadav
Computer Science and Engineering, RGPV,
Bhopal (M.P.), India

Abstract—Network Intrusion detection System (NIDS) is an intrusion detection system that tries to discover malicious activity such as service attacks, port scans or even attempts to break into computers by monitoring network traffic. Data mining techniques make it possible to search large amounts of data for characteristic rules and patterns. If applied to network monitoring data recorded on a host or in a network, they can be used to detect intrusions, attacks or anomalies. "Machine learning method", cascading Principal Component Analysis (PCA) and the Q-learning methods to classifying anomalous and normal activities in a computer network is being proposed. This paper investigates the use of PCA to reduce high dimensional data and to improve the predictive performance. On the reduced data, representing a density region of normal or anomaly instances, Q-learning strategies are applied for the creation of agents that can adapt to unknown, complex environments. Attempt has been made to create an agent that would learn to explore an environment and collect the malicious within it. Interesting results obtained where agents were able to re-adapt their learning quickly to the new traffic and network information as compare to the other machine learning method is being presented such as supervised learning and unsupervised learning

Keywords—Intrusion, Anomaly Detection, Data Mining, PCA, Q-learning Feature selection, real-time misuse intrusion detection, network security, component analysis, sensitivity mismatch measure, specificity mismatch measure.

1. INTRODUCTION

Network intrusion detection systems (NIDS) are most efficient way of shielding against network-based attacks intended at computer systems [1, 2]. Basically, there are two main types of intrusion detection systems: signature-based (SBS) and anomaly-based (ABS). SBS systems [3, 4] rely on pattern recognition techniques. ABS systems [5] build a statistical model describing the normal network traffic, and any abnormal action that deviates from the model is recognized. A network anomaly by malicious or unauthorized users can cause harsh interruption to networks. Hence the development of a robust and reliable network anomaly detection system (ADS) is progressively more important. Anomaly Detection System (ADS) monitors the performance of a system and flag major deviations commencing the normal activity as an anomaly. In this work our goal is to make anomaly-based intrusion feasible. In our experiment, we used KDD Cup 1999 dataset [6]. The dataset consisted of 494,021 records single connection vectors each of which contains 41 features. Each record is labeled as either normal or attack type, with precisely one specific attack type. The space and time complexities of largely classifiers used are exponential function of their input vector size [7]. Additionally, the demand for the number of samples for the training the classifier develops exponentially with the dimension of the feature space. This limitation is called the *'curse of dimensionality'*. Pragmatic studies specify that feature reduction technique is capable of reducing the dimension of dataset. In this work we aim to sort out superfluous information and extensively reduce number of computer resources, both memory and CPU time vital to detect attacks. This paper propose Principal Component Analysis (PCA) as a reduction tool and learning algorithm as a learning tool for the developed system, firstly we reduce the features and then apply the learning algorithm. Q-learning will help to identify the unknown attacks [8].

2. INTRUSION DETECTION SYSTEM

Intrusion Detection System (IDS) is software that automates the intrusion detection process and detects possible intrusions. IDS serve three essential security functions: they monitor, detect, and respond to unauthorized activity by insiders and outsider intrusion. An ID is a system for detecting intrusions and reporting them precisely to the suitable authority.

2.1 Types of IDS

These are the following types of Intrusion detection systems:

2.1.1. Network Intrusion Detection System

NIDS examines the behavior of a specified environment and make a decision whether these activities are malicious (intrusive) or legitimate (normal) based on system integrity, confidentiality and the availability of information resources [9]. NIDS does this by reading all incoming packets and endeavoring to find number of TCP connection demands to a huge number of different ports is detected, one could suppose that there is someone conducting a port scans of some or

all of the computers in the network. It typically tries to detect incoming shell codes in the same approach that a usual intrusion detection system does. Frequently examining precious information about an ongoing intrusion can be learned from outgoing or local traffic and also work with other systems as well. For example renew some firewalls blacklist with the IP address of computers used by intruder.

2.1.2. Host-based Intrusion Detection System

Host-based intrusion detection system (HIDS) examines elements of the dynamic behavior and the status of computer system, vigorously inspects the network packets [9]. A HIDS also check that proper regions of memory have not been modified, for example- the system-call table comes to mind for Linux and various v table structures in Microsoft Windows. For each object in question typically remember its attributes and create a checksum of some kind (an MD5, SHA1) for the substances, this information gets stored in a protected database for later comparison (checksum-database). At installation time- whenever any of the observed objects change legitimately- a HIDS have to initialize its checksum database by examining the proper objects. Persons in charge of computer security need to control this process tightly in order to prevent intruders making unauthorized changes to the database.

2.2 IDS Techniques

There are two complementary trends in intrusion detection [10]:

2.2.1. *Misuse detection*

The search for evidence of attacks based on the knowledge collected from known attacks and is referred to as *misuse detection or detection by appearance.*

2.2.2. *Anomaly detection*

The search for deviations from the model of unusual behavior based on the observations of a system during a normal state and is referred to as *anomaly detection or detection by behavior.*

3. DATA MINING TECHNIQUES FOR ADS

Data mining is extracting facts, secret information in large degrees of raw data. Typical tasks of data mining are detecting fraud and abuse in insurance and finance, predict peak load of a network. Hence Data Mining-based anomaly detection is become widespread in essence. Intrusion is an action that tries to destroy that secrecy, integrality and usability of network information, which is unlicensed and exceed authority. Data mining can be supervised, unsupervised supervised or reinforcement learning is to use the available data to build one particular variable of interest in terms of rest of data. Anomaly detection refers to discovering patterns in a given dataset that deviates from an established normal behavior. The patterns as a result detected are called anomalies and turn to critical and actionable information in several application domains. Anomalies are also known as outlier, surprise deviation etc. Anomaly detection algorithms require a set of normal data to train the model and implicitly consider that anomalies can be treated as patterns not observed before. An outlier may be defined as a data point which is very different from the rest of the data, based on some measure; we use several detection methods in order to see how efficiently these methods may deal with the problem of anomaly detection. The statistics community has studied the concept of outliers widely. In these techniques, the data points are modeled using a stochastic distribution and points are verified to be outliers depending upon their relationship with this model. On the other hand with increasing dimensionality, it becomes gradually more difficult and inaccurate to estimate the multidimensional distributions of the data points.

Profile based methods: This method is similar to rule based method but in this profile of normal behavior is built for different types of network traffics, users, and all devices and deviance from these profiles means intrusion.

Statistical based methods: Statistical methods observe the user/network behavior by measuring explicit variables statistics over time [11].

Distance based methods: These methods try to conquer restraints of statistical outlier detection approach when the data are difficult to estimate in the multidimensional distributions [12].

Rule based: Rule based system uses a set of "if-then" implication rules to distinguish computer attacks.

State transition: In this approach IDSs try to indentify intrusion by using a finite state machine that deduced from network. IDS states communicate to dissimilar states of the network and an event make transfer in this finite state machine. An activity identifies intrusion if state transitions in the FSM of network reflect to continuation state.

Model based methods: Other approaches based on deviation normal and abnormal behavior is modeling them but without creating several profile for them .In model based methods, researcher's effort to model the normal and/or abnormal behaviors and divergence from this model means intrusion.

Signature based: Matching available signatures in its database with collected data from activities for identifying intrusions.

Neural Network Based: This Neural Network model solved normal attack patterns and the type of the attack when given data was presented to the model.

4. FEATURE REDUCTION TECHNIQUES

In machine learning and statistics, dimension or feature reduction is the process of reducing the number of random variables under consideration, and can be divided into feature selection and feature extraction. Feature reductions concern with the mapping of the multidimensional space into lower space dimensions [13]. Feature extraction includes features construction, sparse representations, space dimensionality reduction, and feature selection all these techniques are used as pre-processing to machine learning and statistics tasks of prediction, including pattern recognition. Though such problems have been tackled by researchers, there has been recently a renewed interest in feature extraction. The reduced feature space truly contributes to classification that cuts preprocessing costs and minimizes the effects of the 'peaking

phenomenon' in classification [14], thus improving the overall performance of IDS. The frequently used dimensionality reduction techniques consist of supervised approaches such as Linear Discriminant Analysis (LDA), Random projection, unsupervised ones such as Principal Component Analysis (PCA), and added spectral and manifold learning methods. One inadequacy of the supervised methods is that attribute that describe examples of infrequent classes tend to be easily removed as a result of dimensionality reduction making use of the class distribution.

5. PROPOSED ALGORITHM

A NIDS monitor and analyze network traffics, and use multiple sensors for detecting intrusions from internal and external networks. NIDS explores the information assembled by the sensors, and returns a synthesis of the input of the sensors to system administrator or intrusion prevention system. System administrator carries out the instructions organized by the intrusion detection system. In our proposed anomaly based NIDS, two algorithms namely principal component analysis (PCA) and Q-learning are used shown in figure 1. In this approach, firstly dataset dimensions are reduced by the principal component analysis and finally the anomaly is detected from the reduced dataset by Q-learning method. As q-learning is based on off-policy control hence, it gives an optimized result as an output. Principal Component Analysis is used for dimension reduction and Q-learning is used as a classifier of reduced data. The description of PCA and Q-learning are given below.

5.1 Principal Component Analysis (PCA)

In our network intrusion detection system we have used PCA for dataset reduction. For testing the NIDS system we have used KDDCup99 dataset . Initially in KDDCup99 dataset there is 41 attributes. When we apply the PCA on KDDCup99 dataset, it reduces 41 attributes into 26 attributes. PCA is an unsupervised feature selection based on multivariate statistics and its basic scheme is to search for a projection that represents the data in a best possible way in a least-square sense to provide dimensionality reduction. PCA is a useful statistical technique mainly in fields such as face recognition and image compression, and is a common technique for finding patterns in high dimensional data. The intact focus of statistics is based on around the idea that you have this big set of data, and you want to analyze that set terms of the relationships between the individual points in that set. PCA is way of identifying patterns in data, and expressing the data in such a way as to emphasize their similarities and differences.

5.2 Q-learning Technique

One of the most important advances in reinforcement learning was the growth of an off-policy Temporal Difference (TD) control algorithm known as *Q-learning.* It can be used to discover an optimal action-selection mapping, known as policy (π), for finite Markov Decision Process (MDP). It learns an action-value function that finally gives the expected value of taking a given action in a given state and following the optimal policy through agents subsequently. A history of an agent is a sequence of <state – action – reward>. When such an action-value function is learned, the optimal policy can be created by simply selecting the action with the highest value in each state. Q-learning is able to evaluate the expected utility of the available actions without requiring a model of the environment. It can handle problems with stochastic transitions and rewards, without requiring any alterations. Q-learning is an off-policy scheme that can be run on top of any approach wandering in the MDP. It uses the information studied to approximate the optimal function, from which one can construct the optimal policy. Q-learning does converge to the optimal Q function, under very mild conditions and for proofs are present for this [20]. Optimal result depends on three factors i.e. initial condition (*s0, a0*), discount factor ($0 \leq \gamma \leq 1$) and learning rate ($0 < \alpha \leq 1$).

5.3 Neural network methods for feature extraction

In this paper we present two neural network methods (NNPCA and NLCA) to reduce the dimensionality of TCP network traffic through feature extraction. We compare our methods with the traditional matrix method of Principal Component Analysis (PCA) and show that the NLCA and NNPCA perform better than PCA in eliminating redundant information and retaining essential causal and dynamic traits in the data that significantly contribute to decision making in classifier based misuse intrusion detection applications. To experimentally verify the effects of feature extraction on the detection accuracy and false positive rate of a classifier based IDS, we implement misuse detection systems using two classifiers: (1) the Non-linear classifier (NC), and (2) the CART decision tree classifier (DC) for machine discrimination of normal and intrusive network traffic. For our experiments we use the KDD Cup 1999 intrusion detection dataset prepared by Lee et al. The dataset contains 41 features representing selected measurements of normal and intrusive TCP sessions. Each labeled TCP session is either normal or a member of one of the 22 attack classes in the dataset. We report the performance of the classifiers in recognizing TCP session classes in four datasets: (1) the original KDD Cup 1999 dataset with 41 features, (2) the PCA reduced dataset, and (3) the NNPCA reduced dataset, and (4) the NLCA reduced dataset.

In addition to fast and effective reduction of dimensions in the feature space, feature extraction methods for real-time intrusion detection applications should consider changes in the behavior of background traffic workloads and should accommodate new features that may be discovered in near future. In this context, we introduce two properties essential to feature extraction for intrusion detection: (1) the Adaptive Property and (2) the Scaling Property. The first property refers to the ability of the method to adapt to variations in background network or host traffic workloads. This property essentially gives the extraction method the ability to handle burstiness (high variations in background traffic over varying time scales) [14] and non-stationarity inherent in internet traffic. This property also delays the over fitting-like phenomenon in which the approximation function no longer qualities (over a period of time) to transform the data entering the intrusion detection classifier. Thus, the adaptive property contributes to the stability of the subsequent classification process. The second property refers to the ability to incorporate newly identified features while maintaining

minimum retraining costs. PCA is an efficient method to reduce dimensionality by providing a linear map of d-dimensional feature space to a reduced k-dimensional feature space.

However, PCA has high time complexity (which grows at least quadratically with dimensions of data) and lacks the properties of adaptively and scaling that are essential to real-time intrusion detection applications. Alternatively, the neural network approach to dimension reduction using NNPCA and NLCA give instantaneous response to input, adapt to new input patterns and scale to incorporate new features with minimal retraining. To experimentally verify the effects of feature extraction by PCA, NNPCA, and NLCA on the detection accuracy and false positive rate of a subsequent classification process, we implement two classifiers. The first classifier NC was chosen as a representative of conventional distance based statistical pattern recognition capable of yielding non-linear decision boundaries. The second classifier DC was chosen as a representative of nonmetric methods to classification. The results of classifying the original datasets and its low-dimensional counterparts obtained by PCA, NNPCA and NLCA show that the classifiers achieve equivalent and (in some cases) better detection accuracies and false positives using the reduced datasets.

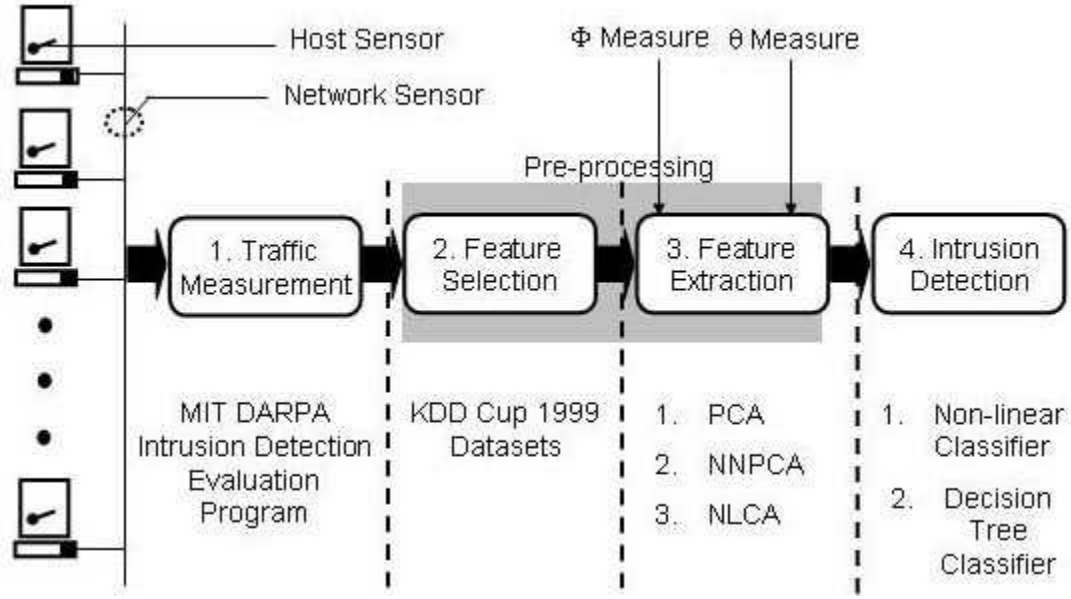

Fig. 1. Four stages of classifier based IDS architecture and their implementation details. The work in this paper contributes to the third stage using PCA, NNPCA, and NLCA methods and fourth stage using NC and DC.

The four stages of a classifier based intrusion detection system are illustrated in Figure 1. The first stage involves measurement of traffic workloads using host and network sensors. Sensors are software programs (e.g., sniffers capturing packets and software utilities monitoring system calls and CPU cycles) that monitor selected characteristics of the host/network traffic. Traffic measurement was done under DARPA Intrusion Detection Evaluation Program . The second stage (preprocessing) involves two tasks. In this paper we perform the second task of feature extraction by using the 10% subset of KDD Cup 1999 dataset for identifying key features that contribute to classifier based misuse detection. The dataset contains approximately 500,000 TCP sessions. Each session contains 41 selected measurements of TCP connections and is labeled either as an attack or a non-attack. The final stage involves attack detection for which we use NC and DC classifiers.

5.3.1 Component Analysis

Component analysis is an unsupervised approach to find significant features in the data. In this section we discuss three component analysis techniques (1) PCA, (2) NNPCA, and (3) NLCA for reducing dimensionality of KDD Cup 1999 intrusion detection dataset. The dataset contains 41 features of TCP traffic. Each feature vector is labeled as an attack or a non-attack. There are 22 types of attacks in the dataset. We divide the dataset into training data subset (containing 25% of randomly selected representative samples from the original dataset) and reserve the rest for testing. On performing component analysis on the training subset, we obtain three compressed datasets in addition to the original dataset. Table I summarizes the four datasets later used for misuse detection using NC and DC.

TABLE I
Summary of datasets obtained after feature extraction.

Dataset Name	Reduced Dimensions	Method
ORIGDATA	41	None
PCADATA	19	PCA
NNPCADATA	19	NNPCA
NLCADATA	12	NLCA

PCA

Principal Component Analysis reduces the dimensionality of data by restricting attention to those directions in the feature space in which the variance is greatest. In PCA, the proportion of the total variance accounted for by a feature is proportional to its eigenvalue. We perform PCA on 25% training data subset. Here, the goal is to reduce the cardinality of the dimensions (d) in the data where d = 41. We excluded two features (1) number of outbound commands and (2) is host login as their values remained constant throughout the dataset, reducing d to 39. We compute the correlation matrix for the training dataset. Next, we compute the eigenvalues and sort them in decreasing order. The first eigenvalue e1 corresponds to the first principal component, the second eigenvalue e2 corresponds to the second principal component and so on. Table II shows the _first 20 eigenvalues arranged in decreasing order. We use two tests: (1) Screen Plot test and (2) Critical Eigenvalue test as a test of hypothesis that k features are sufficient against the alternative that more than k features are required. The remaining d-k features are assumed to contain noise or redundancy. In Screen Plot test, we plot the principal components against the differences mi in successive sorted eigenvalues (e.g., mi = ei - ei+1).

6. EXPERIMENT AND RESULTS

Test Data: The training set employed for this analysis is the "10% KDD" (kddcup_data_gz file) dataset and converted into excel form or in matrix form. It consists of 41 feature attributes out of which 3 are symbolic and 38 are numeric. Hence each connection is given by 41 features set. There are 65536 sample of connection described in 41 dimensions, from which 39298 are normal and 26238 are attacks. The 42nd field can be a label generalized as Normal, DoS, Probing, U2R, and R2L. The training data is made up of 22 different attacks. The known attack types are those present in the training dataset while the novel attacks are those attacks which are present in the test datasets but not available in the training datasets. Generally, there are four categories of attacks. They are:

DoS (denial-of-service), for example, ping- of death, syn flood, etc.

Probe, surveillance and probing, for example, port-scan, ping-sweep, etc.

R2L, unauthorized access from a remote machine, for example, is guessing password.

U2R, unauthorized access to local super user rights by a local unprivileged user, for example, various buffer overflow attacks.

Training data: 10% of training data is selected randomly from the 10% of kddcup'99 dataset. Training data contains half the no. of normal data and half of the abnormal data, i.e. 3600 samples for each.

Performance Evaluation and Results

We are emphasizing on the following performance measures which are considered to evaluate the efficiency of the Proposed IDS technique: The true positive rate (TPR) is the proportion of examples which were classified as class x, among all examples which truly have class x, i.e. how much part of class was captured. It is equivalent to detection rate or sensitivity. In case of information recovery, it is called as Recall. The false positive rate (FPR) , which is also known as false alarm rate is the proportion of examples which were classified as class x, but belong to a different class, among all examples which are not of class x.

Precision is another information retrieval term, which is often paired with recall. It is defined as the proportion of examples which truly have class x among all those which were classified as class x. F-value combines the TPR and precision into a single value function after obtaining their harmonic mean. Building time is the time taken by the classifier to build the model in seconds. While experimenting on different threshold values in the proposed IDS technique, we got the results of the parameters.

7. CONCLUSION AND FUTURE WORK

In this paper a general unsupervised (PCA) and reinforcement learning (Q-learning) methods have been used for classifying anomaly instance in large and complex network datasets. An explanation mechanism to explain the normal or anomalies results was explained. The precise approaches of the anomaly based detection systems learning are characterized. Based on cascading two machine learning techniques i) Principal Component Analysis and, ii) the Q-learning, we developed an anomaly based network intrusion detection technique. Firstly Principal Component Analysis (PCA) is used to reduce the features of KDDCup99. Then we have applied the learning algorithm, Q-learning to identify the novel and complex attacks decision space into classification regions; there by improving the system classification performance. Our future direction is to employ dataset as a tuple to this anomaly based network intrusion detection technique to increase the different measuring parameters. We have developed signed quantitative measures GI, , and Θ to test the performance of feature extractors in intrusion detection applications. We use these measures to evaluate the performance of PCA, NNPCA, and NLCA feature extractors on misuse detection systems employing nonlinear and decision tree classifiers. We show that the neural network feature extraction methods are more effective than PCA in reducing dimensions and retaining the causal dynamic information that is essential for maintaining high detection accuracy and low false positive rate in misuse detection systems. We are extending our work on quantitative measures to find optimal combinations of classifiers and feature extractors for intrusion detection systems.

REFERENCES

[1] Hazem M. El-Bakry, Nikos MastorakisA, "Real-Time Intrusion Detection Algorithm for Network Security,WSEAS Transactions on communications, Issue 12, Volume 7, December 2008.

[2] Debar.H, Dacier.M and Wespi.A, "A Revised Taxonomy of Intrusion-Detection Systems" Annales des Telecommunications 55(7–8) (2000) 361–378.

[3] Roesch.M, "Snort - Lightweight Intrusion Detection for Networks" 13th USENIX Conference on System Administration, USENIX Association (1999) 229–238.
[4] Sourcefire: Snort Network Intrusion Detection System web site (1999) URL http://www.snort.org.
[5] Wang. K and Stolfo.S.J, "Anomalous Payload-Based Network Intrusion Detection" 7th Symposium on Recent Advances in Intrusion Detection, Volume 3224 of LNCS., Springer-Verlag (2004) 203–222
[6] KDDcup99, Dataset: kdd.ics.uci.edu/databases/kddcup99/kddcup99.htm
[7] R.O.Duda,P.E.Hart, and D.G.Stork, Pattern Classification, vol. 1. New York: Wiley, 2002
[8] Watkins,C. Learning from Delayed Rewards, Thesis, University of Cambridge, England 1989.
[9]. A. Macgregor, M.Hall, P.Lorier and J.Bruskill, "Flow clustering using machine learning techniques", In PAM 2004, Antibes-Juan-Les-Pins, France, LNCS. pp. 205-214, 2004.
[10] S. Kumar, Classification and Detection of ComputerIntrusions, Ph.D. Thesis, Purdue University.
[11] White paper, Intrusion Detection: A Survey,ch.2, DAAD19-01, NSF, 2002
[12] K. Scarfone, P. Mell, Feb. 2007. Guide to Intrusion Detection and Prevention Systems (IDPS), NIST Special Publication, 800-94.
[13] Gopi K. Kuchimanchi,Vir V. Phoha, Kiran S.Balagani, Shekhar R.Gaddam, Dimension Reduction Using Feature Extraction Methods for Real-time Misuse Detection Systems, Proceedings of the IEEE on Information, 2004.
[14] Anil K. Jain,Robert P.W. Duin, and Jianchang Mao,"Statistical Pattern Recognition" IEEE transactions on pattern analysis and machine intelligence, VOL. 22, NO. 1,January 2000.

