Neurocomputing 164 (2015) 71–81

Contents lists available at ScienceDirect

Neurocomputing

journal homepage: www.elsevier.com/locate/neucom

PCA filtering and probabilistic SOM for network intrusion detection

Eduardo De la Hoz [a], Emiro De La Hoz [a], Andrés Ortiz [b,*], Julio Ortega [c], Beatriz Prieto [c]

[a] Programa de Ingeniería de Sistemas, Universidad de la Costa, Barranquilla, Colombia
[b] Communications Engineering Department, University of Málaga, Spain
[c] Computer Architecture and Technology Department, CITIC, University of Granada, Spain

ARTICLE INFO

Article history:
Received 11 January 2014
Received in revised form
15 August 2014
Accepted 21 September 2014
Available online 13 March 2015

Keywords:
Probabilistic SOM
Bayesian SOM
IDS
Self-organizing maps
PCA filtering

ABSTRACT

The growth of the Internet and, consequently, the number of interconnected computers, has exposed significant amounts of information to intruders and attackers. Firewalls aim to detect violations according to a predefined rule-set and usually block potentially dangerous incoming traffic. However, with the evolution of attack techniques, it is more difficult to distinguish anomalies from normal traffic. Different detection approaches have been proposed, including the use of machine learning techniques based on neural models such as Self-Organizing Maps (SOMs). In this paper, we present a classification approach that hybridizes statistical techniques and SOM for network anomaly detection. Thus, while Principal Component Analysis (PCA) and Fisher Discriminant Ratio (FDR) have been considered for feature selection and noise removal, Probabilistic Self-Organizing Maps (PSOM) aim to model the feature space and enable distinguishing between normal and anomalous connections. The detection capabilities of the proposed system can be modified without retraining the map, but only by modifying the units activation probabilities. This deals with fast implementations of Intrusion Detection Systems (IDS) necessary to cope with current link bandwidths.

© 2015 Elsevier B.V. All rights reserved.

1. Introduction

Nowadays, with the growth of Internet, not only the number of interconnected computers, but also the relevance of network applications, has increased considerably. At the same time, the trend to online services has exposed sensitive information to intruders and attackers [16,3]. Common protection approaches do not react to attackers or intruders, but only suppose a passive position to reduce exposure. On the other hand, the complexity of the newer attacks necessitates the use of elaborated techniques, such as pattern classification or artificial intelligence, for successfully detecting an attack or just to differentiate among normal and anomalous traffic. Other approaches that implement an active protection against real or potential attackers include firewall-like systems capable of inspecting data packets. IDS and Intrusion Protection Systems (IPS) are active systems that continuously monitor the network. These systems calculate some features from the monitored network in order to classify the traffic, detect abnormal behaviours and react according to predefined rules. This presents a classification problem, with some requirements needing specific approaches, thus contributing to the machine learning field.

There are two IDS design approaches [3,15,27,17] depending on the detection philosophy. The first is the so-called *signature-based* IDS [27], which analyses all the incoming packets looking for known patterns associated with intrusion attempts. These patterns are stored in a database and can be compared with patterns extracted from incoming network traffic. In other words, signature-based IDS works similarly to virus scanners as they also compare observed behaviours with stored ones. However, this method is not able to detect attacks whose signature is not in the database. Similarly, outdated databases or deficient signatures may cause false negatives or false positives (that is, missing an actual attack or misreading legitimate traffic as an attacker). The second searches for deviations from normal patterns to decide whether a connection is classified as anomalous, namely *anomaly-based* [17]. These systems usually characterize normal patterns by means of statistical learning techniques applied to network traffic. In addition, using complex features allows discovering not only an actual intrusion, but also a potential one, namely *anomaly-based* IDS. Nevertheless, in *anomaly-based* systems, sufficiently accurate models are necessary to distinguish normal from abnormal patterns. Otherwise, the IDS is likely to generate too many false positives or negatives. *Anomaly-based* IDS can be addressed, for instance, by discovering a misuse of the protocol flags or an abnormal number of certain events (such as the

* Corresponding author. Tel.: +34 952133353.
E-mail addresses: edelahoz6@cuc.edu.co (E. De la Hoz), edelahoz@cuc.edu.co (E. De La Hoz), aortiz@ic.uma.es (A. Ortiz), jortega@ugr.es (J. Ortega), beap@ugr.es (B. Prieto).

http://dx.doi.org/10.1016/j.neucom.2014.09.083
0925-2312/© 2015 Elsevier B.V. All rights reserved.

number of TCP connection attempts). Nevertheless, due to attack diversity, it is necessary to compute more complex features to improve detection.

In the last years, different intrusion detection approaches have been proposed, including the use of artificial intelligence techniques, such as neural networks [55].

As explained in the next section, anomaly detection is not a straightforward task in a real environment [42,29,49,15] and poses interesting problems related to classification and feature selection.

This way, datasets such as KDD99 (and also the NSL-KDD) have been built to provide training and test subsets with different statistical distributions as expected in real anomaly detection tasks. As the KDD99 is a large-volume dataset, researchers usually take random samples for their experiments that explain the discrepancies observed in the literature [58]. In [37], an analysis is provided of the low level of industry adoption of intrusion detection procedures proposed in the academic literature, despite their reported high performance. Among those reasons, incorrect feature selection procedures and statistical analysis, as well as not having enough detailed experiments, are considered. In this paper, the IDS concerns expressed in [37] have been taken into account and addressed.

In this work, Principal Component Analysis (PCA) is used to generate a new set of non-correlated features in order to remove noise and to avoid using low variance variables (that is, almost single-valued variables). Moreover, these new features are selected according to their discriminative capability. Subsequently, feature space modelling and classification is addressed by means of Probabilistic SOM, a fuzzy version of classical SOM that allows measuring the activation probability of each unit. Nevertheless, detecting not only an attack but also the type is not a straightforward task, and previous approaches have not been able to obtain high per attack detection accuracy values [42,29].

The rest of the paper describes the databases and methods used in this work, and the experimental results. Specifically, Section 2 is split into three subsections, feature filtering and selection procedures (Sections 2.1 and 2.2), and the use of probabilistic SOM for modelling and classification (Section 2.3). Then Section 3 describes the dataset used for the experiments and the feature selection accomplished to distinguish between anomalies and normal traffic. Finally, Section 4 analyses the previous work done in this line and Section 5 summarizes the conclusions of the paper.

2. Proposed methods

The proposed feature selection and classification method for anomaly detection is presented in this section, which has been split into three subsections that summarize our approach. Fig. 1 shows its corresponding block diagram.

2.1. Feature generation and PCA filtering

Feature selection is a key step in classification problems as it contributes to removing redundant or irrelevant input features not only to reduce computing times for learning, but also to improve classifier accuracy [58]. The methods for feature selection can be classified into filter, wrapper and hybrid methods. Filter methods select the feature subset as a pre-processing step according to a chosen criterion and without taking into account the performance of the classifier. Thus, filter methods are usually less computational than expensive wrapper methods that use the classification outcomes to evaluate the feature selection methods. Although wrapper methods usually outperform filter methods with respect to classifier accuracy, the results obtained are usually not applicable whenever the classifier is changed. Thus, there are proposals

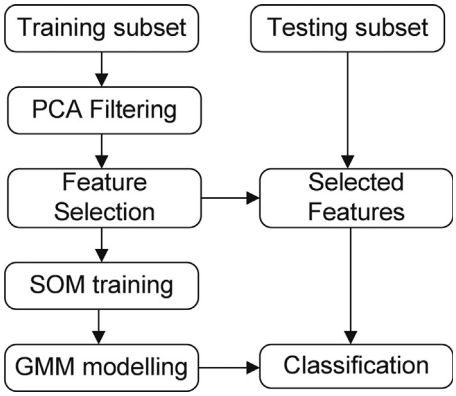

Fig. 1. Block diagram of the proposed anomaly detection system.

(that is, hybrid methods) that combine a wrapper method with a filter that guides the classifier. The approach considered in this paper can be included in the filter methods.

Principal Component Analysis (PCA) has been widely used in many applications for extracting the most relevant dataset information. In fact, it has been successfully used in face recognition applications [51]. In this case, PCA is used to derive a new set of uncorrelated features from a set of correlated ones. Thus, PCA generates a set of orthogonal basis vectors so that the data can be expressed as a linear combination of that basis. Some papers [14] have claimed that this method presents some classification task problems as it requires more processing whenever new data is added and it is not invariant under a transformation of the data.

The procedure can be explained as follows. Let $X=\{\mathbf{x}_1,\ldots,\mathbf{x}_{N_t}\}$, $\mathbf{x_i}=(x_i^1,\ldots,x_i^n)^T$ be the input data samples (training samples). A shifted version of the data manifold can be obtained by subtracting the mean ($\overline{X}$), $Y=X-\overline{X}$, where $\mathbf{y}_i\in\mathbb{R}^n$, $\mathbf{y}_i=(y_i^1,\ldots,y_i^n)^T$, $i=1,\ldots,N_t$. PCA searches for N_t orthonormal vectors $\mathbf{u}_k=(u_k^1,\ldots,u_k^n), k=1,\ldots,N_t$ such that

$$\lambda_k=\frac{1}{M}\sum_{r=1}^{N_t}(\mathbf{u}_k^T\mathbf{y}_r)^2 \tag{1}$$

is maximum. Vectors $\mathbf{u}_k$, $k=1,\ldots,N_t$ verify that $\mathbf{u}_l^T\mathbf{u}_k=\delta_{lk}$ (δ_{lk} is the Kronecker delta). Vectors $\mathbf{u}_k$ and scalars λ_k are the eigenvectors and eigenvalues, respectively, of the covariance matrix computed as $C=YY^T$. It is worth noting the difference between the presented method and the *eigenconnections* approach [5], inspired by the face recognition method using eigenvectors (*eigenfaces*) [51] due to its appearance. In this case, eigenvectors are used to generate a new feature space that allows us to remove noise comprising the discriminative information in a reduced number of features. Thus, the training data samples are projected onto the space spanned by the *eigenvectors* to generate a set of uncorrelated features that best describe the data manifold. These features are further used to train the SOM-based classifier described in this section. In order to classify a new data instance $\mathbf{v}$, it has to be projected onto the *eigenvectors* space, obtaining its corresponding feature vector:

$$\boldsymbol{\omega}_k=(\mathbf{v}-\overline{X})*\mathbf{u}_k \tag{2}$$

On the other hand, the original data can be reconstructed from the principal components as

$$\mathbf{v}_k^{rec}=\overline{X}+\boldsymbol{\omega}_k*\mathbf{u}_k^T \tag{3}$$

where v_k^{rec} is the reconstruction of $\mathbf{v}$ using the eigenvector k. Although in the problem considered in this work, the two first principal components account for more than 95 percent of the variance, it does not ensure the discriminative capability of the projections. Thus, selected eigenvectors are sorted by their

Download English Version:

https://daneshyari.com/en/article/406428

Download Persian Version:

https://daneshyari.com/article/406428

Daneshyari.com