Anomaly detection using forecasting methods
ARIMA and HWDS

Eduardo H. M. Pena, Marcos V. O. de Assis, Mario Lemes Proença Jr.
Computer Science Department
State University of Londrina, Londrina, Brazil
Emails: {eduardohmpena, mvoassis}@gmail.com, proenca@uel.br

Abstract—Understanding the normal operation of IP networks is a common step in building a solution for automatic detection of network anomalies. Toward this end, we analyze the usage of two different approaches: the AutoRegressive Integrated Moving Average (ARIMA) model and an improvement of the traditional Holt-winters method. We use both models for traffic characterization, called Digital Signature of Network Segment using Flow analysis (DSNSF), and volume anomaly or outliers detection. The DSNSFs obtained by the presented models are compared to the actual traffic of bits and packets of a real network environment and then subjected to specific evaluations in order to measure its accuracy. The presented models are capable of providing feedback through its predictive capabilities and hence provide an early warning system.

I. INTRODUCTION

Networks and distributed processing systems have become an essential technology in any Enterprise Environment. The rapid growth of the amount of data that those environments have to deal has given rise to a depletion in expertise of human operators to manage them. A lot of efforts has gone into developing systems and protocols for collecting network traffic statistics and most of the work in the network management architecture focuses on defining detailed network traffic objects. Relatively, a limited number of researches were made aiming to support user perception of collected statistics, with most of the analysis being left to the common-sense of network operators. Thus the need to develop automated, accurate and reliable network management systems is essential. A significant problem related to network management is anomalies detection. Anomalies are unusual and significant changes in a network's traffic levels. Regardless of whether the traffic anomalies nature are malicious or unintentional, it is important to analyze them since they can create congestion in the network and deplete the available bandwidth resources, having a significant impact on the end user. We assume that anomalies induce changes in the characteristics of the network traffic, but we do not require these anomalies to be known a priori.

Many important contributions have been proposed for anomalies detection in network traffic. Clustering methods [1], entropy-based methods [2], Haar-wavelet analysis [3], association rule mining [4], principal component analysis (PCA)[5], etc. In this paper we address the problem of traffic characterization and detection of traffic anomalies using sFlow analysis by incorporating two different models into a behavior based system. The first is the AutoRegressive Integrated Moving Average (ARIMA) model [6], which is a linear time series forecasting model that captures the linear dependency of the future values on the previous data. The second is the use of an improvement of the Holt-Winters statistical forecasting model, called Holt-Winters for Digital Signature (HWDS) [7]. Each model were chosen due to their ability to forecast the future traffic rate based on measured traffic history. The models have similar components, as they are time series forecasting techniques, based on trend and seasonality.

Some of the advantages of both models is that in principle they are not restricted to any specific environment, and that they provide a way of detecting unknown attacks. The anomaly detection performance is directly correlated with the traffic prediction traffic methods ARIMA and HWDS, and, therefore, they need to be accurate. By using ARIMA and HWDS models, we can predict the future trend of the normal network’s behavior. The forecasted behavior (traffic characterization) is called Digital Signature of Network Segment using Flow analysis (DSNSF), which is used on the detection of volume anomalies.

II. ARIMA PROCESS

Some ARIMA processes in network security applications are presented in [6] and [8]. Both works relied on simulated data to emulate a real network environment and also for synthetic generation of anomalies. The usage of ARIMA processes in network behavior characterizing and anomaly detection usually assumes that the ARIMA parameters are properly learned, comparing data segments with those predicted through the model to determine anomalies occurrences. Our modeling relies on real network traffic data from a university and investigates the presence of anomalies using the built DSNSF.

An ARIMA process may be generalized in equation 1:

$$z_t - \sum_{i=1}^{p} \phi_i z_{t-i} = e_t - \sum_{j=1}^{q} \theta_j z_{t-j},$$

where $e_t$ is the forecast error at time $t$, $\phi$ and $\theta$ are the autoregressives and moving average coefficients of finite order $p$, $q$, respectively. Yet, the original time series is differentiated $d$ times in order to obtain $z_t$, the Integrated part of the model.
The creation of Digital Signature of Network Segment using Flow analysis (DSNSF) from the ARIMA model occurs dynamically using the past weeks data for training and the changes in every new day processed to recalibrate the model. Some standard techniques are available for parameter estimation [9].

III. Holt-Winters for Digital Signature (HWDS)

Holt-Winters is a statistical forecasting model applied to time series characterized by the presence of seasonality (periodicity) and linear trend, based on the Exponential Weight Moving Average method (EWMA). This model divides the analyzed data in three parts, each being represented by an equation of the EWMA type. They are the baseline, the linear trend and the seasonality trend. In this paper we use an improvement of the traditional Holt-Winters method called Holt-Winters for Digital Signature (HWDS)[7], which modifies the equations that describes the baseline and linear trend in order to achieve better results on the traffic characterization.

IV. Generation of DSNSF and Anomaly Detection Schema

The DSNSFs were generated using the bl-7 methodology, introduced by [10], in which a DSNSF is generated for each workday, based on the history of its previous weeks. In this work, we use a data set consisting of six weeks of 2012 for the creation and evaluation of the DSNSFs. Flows belonging to September are used for ARIMA and HWDS training, whereas data from the 1st to 12th of October are used to measure the effectiveness of the DSNSFs traffic characterization and the alarm system. We use the presented methods to create two DSNSFs for each workday relating to the attributes bits/s and packets/s and compare them with the real traffic observed. Furthermore, the collected data were analyzed in one minute intervals, generating 1440 different intervals each day.

The DSNSFs generated using ARIMA and HWDS are considered as the expected forecasted normal traffic volume. Any deviation over the confidence bands from the predicted value, for the two attributes simultaneously, will be considered as an anomaly. If the pattern is stable enough, the predicted traffic should match the normal traffic accurately. A symmetric approach for the confidence bands creation is employed in ARIMA modeling through the use of variance and mean measures of the calculated DSNSF. For HWDS an asymmetric approach is used, with the intervals where the error between the DSNSF and real data is predominantly superior are updated with the absolute deviation of the interval. The oposed threshold is updated with the standard deviation of the forecast.

V. Results Obtained

We explored two evaluation techniques to measure the effectiveness of the presented models in generating DSNSFs. The first technique used for evaluation of the DSNSFs is the correlation. The results obtained through this calculation vary between -1 and 1, where 1 indicates the total correlation, 0 indicates a null correlation and -1 indicates an inverse total correlation. For accuracy analysis of time series predictions, it is used the Symmetric Mean Absolute Percentage Error (sMAPE), which considers the errors in a symmetrical way, allowing a better analysis of the obtained outcomes. The result of this measure is a percentage error value. In the analyzed scenario, it was observed that sMAPE values between 0% and 15% represent very good forecasts, while values between 15% and 20% describe relatively good predictions on the average.

The correlation and sMAPE tests showed the adaptability to the network traffic, with correlation indices higher than 0.78 and percentage errors between 5% and 20% in most of the cases for ARIMA and HWDS. Table I shows the average results for both evaluation tests.

The anomaly detection schema, an example in Figure 1, enabled the volume traffic faults to be detected by raising the alarms for the periods which the real traffic showed the most significant changes from the DSNSF. The accuracy rates obtained remained in an average of 80% for ARIMA and 89%
TABLE I
TRAFFIC CHARACTERIZATION EVALUATION

<table>
<thead>
<tr>
<th></th>
<th>sMAPE</th>
<th>Correlation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Bits</td>
<td>Packets</td>
</tr>
<tr>
<td>ARIMA</td>
<td>11%</td>
<td>10%</td>
</tr>
<tr>
<td>HWDS</td>
<td>11%</td>
<td>6%</td>
</tr>
</tbody>
</table>

Fig. 3. Correlation test for workdays from 1st to 12th, October

Fig. 4. sMAPE test for workdays from 1st to 12th, October

for HWDS.

To facilitate the outcome analysis of true-positive and false-positive rates, we used the Receiver Operating Characteristic (ROC) curve. This technique makes possible to graphically visualize the correlation between the True-positive rate (TPR) and False-positive rate (FPR) relating to the anomaly detection schema. Its results can be visualized in Fig. 2. When it comes to the correlation between the a true-positive and false positive rates, ARIMA achieved a true-positive rate of 94% with false positive rates of 10% while HWDS achieved rates of 94% and 6% for true-positive and false-positive, respectively.

This difference showed that the confidence bands calculus approaches have a substantial impact in the anomaly detection outcome.

VI. CONCLUSION

In this paper, we present two models to characterize the network traffic and detect anomalies, by identifying patterns and behaviors to create a Digital Signature of Network Segment using Flow analysis (DSNSF) and then compare to actual traffic of the environment tested. The use of the DNSSF proved to be a great tool to model the network behavior since the real traffic of the days followed, most of the time, the characterization calculated by the discussed models: AutoRegressive Integrated Moving Average (ARIMA) and Holt-Winters for Digital Signature (HWDS). We explored two evaluation techniques to measure the effectiveness of the presented methods in generating DNSSFs. The correlation and sMAPE tests showed the adaptability to the network traffic. The anomaly detection schema enabled the volume traffic faults to be detected by raising the alarms for the periods which the real traffic showed the most significant changes from the DNSSF. The use of ARIMA and HWDS obtained good results in traffic characterization as well as in anomaly detection and presents powerful and innovative approaches for efficient management of real networks. Furthermore, the presented models does not require any a prior knowledge of the anomalies to detect suspicious events. In future projects, we intend to test our model in different scenarios, compare the ARIMA and HWDS models with others currently used for traffic characterization, increase the amount of analyzed flow’s attributes and explore the correlation between other parameters and attributes for more effective use of the DNSSF approach.

REFERENCES