2016 Joint International Conference on Service Science, Management and Engineering (SSME 2016) and
International Conference on Information Science and Technology (IST 2016)
ISBN: 978-1-60595-379-3

A Real-Time Detection Approach to Network Traffic Anomalies in Communication Networks

Fan-Bo MENG[1,a,*], Nan JIANG[2], Bo LIU[2], Ran LI[3], Fei XIA[4]

[1]State Grid Liaoning Electric Power Company Limited, Shenyang 110006, China

[2]State Grid Huludao Electric Power Supply Company, Huludao 125000, China

[3]State Grid Shenyang Electric Power Supply Company, Shenyang 110003, China

[4]State Grid Liaoyang Electric Power Supply Company, Liaoyang 111000, China

[a]amengfb@163.com

[*]Corresponding author

Keywords: End-to-end network traffic, Anomaly detection, Principal component analysis, Empirical mode decomposition.

Abstract. With the advance of new network technologies, new types of applications are quickly arising. Network traffic exponentially is rising. Accordingly, this results in new challenges for network traffic anomaly detections. This paper proposes a new quick detection approach to network traffic anomalies. Firstly, network traffic is regarded as a time series of signals and is constructed into a matrix. Secondly, the principal component decomposition is performed for the matrix. The network traffic is divided into principal and non-principal components. Thirdly, the empirical mode decomposition is carried out for these two components. In this case, a quick anomaly detection algorithm is presented. Simulation results show that our approach is feasible and promising.

Introduction

With the rapid development of new network technologies, network applications exhibit new traffic types and this results in network traffic quickly rising. In this case, new network traffic anomalies quickly appears in communication networks. Network traffic anomalies have impact on network performance and users' experience quality [1-2]. How to effectively and efficiently detect and diagnose abnormal and anomalous components in network traffic has become a larger challenge [3-4]. More importantly, anomalous network traffic implies users' and network devices' abnormal or anomalous behaviors. Through detecting the anomalous network traffic, operators can effectively perform active defense for their networks. Therefore, network traffic anomaly detections are very significant in current network operations, which has become a very import research topic at present. This has received very extensive attentions from academic and industrial communities [5-8].

Anomaly detections about network traffic are studied extensively. The time-frequency domain method was proposed to find anomalous components in network traffic [1, 5,9]. They attained the fairly accurate detection results for abnormal network traffic. Information metrics [2] and empirical mode decompositions [3] were used to perform the correct detections of network traffic. In this way, network traffic features were extracted via different metrics or mode functions. The parameter-based detection method was proposed to find the abnormal part of aggregate network traffic [10]. For self-similar network traffic, periodicity features were exploited to extract traffic anomalies [6]. In such a case, network traffic was described as a period signals to model network traffic due to self-similar nature. Additionally, a new detection method was presented to find the abnormal part of network traffic for multimedia applications [7]. Their method could effectively find out and recognize anomalous network traffic. Through modeling network events, a model-based detection approach was proposed to find out abnormal situations in networks [11]. To more effectively and accurately detect

anomalous network traffic, the spectral kurtosis analysis was proposed to recognize and diagnose abnormal parts in network traffic [12]. Dynamic anomaly detection approaches were proposed to identify abnormal parts of dynamic environments [4]. The information theory could effectively used to characterize network traffic [13]. This motivates us to use the signal processing technologies to detect network traffic anomalies.

Different from these methods, this paper proposes a new quick detection approach to find out the anomaly components in network traffic, which combines the principal component analysis with the empirical mode decomposition method. Firstly, we take network traffic as a time series of signals, which is used to construct a traffic matrix. Secondly, the principal component decomposition is performed for the traffic matrix. In this way, the network traffic is divided into principal and non-principal components, in which principal components denotes the principal features in network traffic while non-principal components describe the secondary features in network traffic. Thirdly, we exploit the empirical mode decomposition to decompose these two components. Then the different empirical mode functions are constructed to capture and characterize them, respectively. In this case, we can effectively describe the features of network traffic. At the same time, according to our derivation, a quick anomaly detection algorithm is presented to perform the accurate recognition of anomalous network traffic. Simulation results show that our approach is feasible and promising

The rest of this paper is organized as follows. Our method is derived in Section 2. Section 3 presents the simulation results and analysis. We then conclude our work in Section 4.

Problem Statement

For any network traffic, we can take it as a time signal. Assume network traffic $y(t)$ at time t, and then a time series $y = \{y(t) \mid t = 1,2,...\}$ represents any network traffic over the time. Without loss of generality, assume a network traffic $\tilde{y} = \{y(t) \mid t = 1,2,...,N\}$ with the length by $N = n^2$ where n is an integer. Network traffic $\tilde{y}$ can be converted into the following matrix:

$$Y = \{y_{ij}\}_{n\times n} = \begin{Bmatrix} y(1), & y(2), & ..., y(n) \\ y(n+1), & y(n+2), & ..., y(2n) \\ ... & & \\ y((n-1)^2+1), & y((n-1)^2+2), & ..., y(n^2) \end{Bmatrix} \quad (1)$$

Next, we perform the principal component decomposition for network traffic Y in Equation (1). According to the principal component analysis theory, Y can be decomposed as the following equation:

$$Y = \{y_{ij}\}_{n\times n} = UDV^T \quad (2)$$

We select the k top principal components in network traffic, and then the below equation can be attained:

$$Y_p = \{y_{ij,p}\}_{n\times n} = V^{'}D^{'}U^{'} \quad (3)$$

where $V^{'}$ and $D^{'}$ describe the principal features in network traffic. The model in Equation (3) can be used to characterize the features of network traffic.

Accordingly, according to Equation (3), we perform the converse transformation of Equation (1). In this way, a new time series can be obtained as follows:

$$\tilde{y}_p = \{\tilde{y}_p(t) \mid t = 1,2,...,N\} = \{y_{11,p}, y_{12,p}, ..., y_{nn,p}\}, \quad (4)$$

where $\tilde{y}_p$ characterizes the principal component features in network traffic $\tilde{y}$.

Then another time series $\tilde{y}_{np}$ describing the non-principal component feature in network traffic $\tilde{y}$ can be denoted as:

$$\tilde{y}_{np} = \{\tilde{y}_{np}(t) \mid t = 1,2,...,N\} = \tilde{y} - \tilde{y}_p \tag{5}$$

In this case, network traffic is divided into two parts $\tilde{y}_p$ and $\tilde{y}_{np}$. Now we use the empirical mode decomposition method to extract the features in $\tilde{y}_p$ and $\tilde{y}_{np}$, respectively. As mentioned in [3], we exploit empirical mode decompositions to split network traffic into different intrinsic mode function components. In this case, each intrinsic mode function component reflects the true hidden information in network traffic, and each intrinsic mode function component is mutually orthogonal. Accordingly, we use the empirical mode decomposition to convert network traffic into the orthogonal intrinsic mode function components.

Therefore, for $\tilde{y}_p = \{\tilde{y}_p(t) \mid t = 1,2,...,N\}$ denoting the principal features of network traffic, according to the empirical mode decomposition method, we attain the below equation:

$$\tilde{y}_p(t) = \sum_{i=1}^{m} g_{i,p}(t) + r_{m,p}(t) \tag{6}$$

where $r_{m,p}$ is the residue component which represents the average trend of $\tilde{y}_p(t)$.

Similarly, or $\tilde{y}_{np} = \{\tilde{y}_{np}(t) \mid t = 1,2,...,N\}$ denoting the non-principal features of network traffic, the following equation is attained:

$$\tilde{y}_{np}(t) = \sum_{i=1}^{m} h_{i,np}(t) + s_{m,np}(t) \tag{7}$$

where $s_{m,np}$ is the residue component which represents the average trend of $\tilde{y}_{np}$.

Now, we propose our detection algorithm. The steps of our algorithm is as follows:

Step 1: Give network traffic $\tilde{y} = \{y(t) \mid t = 1,2,...,N\}$, the number *k* of top principal components in network traffic.

Step 2: According to Equation (1), attain traffic matrix Y.

Step 3: According to Equations (2)-(5), network traffic $\tilde{y}$ is decomposed into $\tilde{y}_p$ and $\tilde{y}_{np}$ via the principal component analysis method. Set $r_0(t) = \tilde{y}_p(t)$ and $p = 1$.

Step 4: Set $i = 1$, and initialize the threshold a and the maximum iterative step S.

Step 5: Initialize $k = 0$, $e_{i+1,k}(t) = r_i(t)$, and set the spline function $s(t)$ be a cubic spline, $s = 3$, $v = P$ and $P \gg 0$.

Step 6: Find out local maxima and minima of $e_{i+1,k}(t)$, use a $s(t)$-based spline interpolation method to create two spline curves $s_u(t)$ and $s_l(t)$, get $m_{i+1,k} = (s_u(t) + s_l(t))/2$, and set $e_{i+1,k+1}(t) = e_{i+1,k}(t) - m_{i+1,k}$.

Step 7: If $e_{i+1,k+1}(t)$ satisfies the conditions of an intrinsic mode function component, go to Step 11.

Step 8: If $v > m_{i+1,k}$, set $v = m_{i+1,k}$ and $e(t) = e_{i+1,k+1}(t)$.

Step 9: if $s = 3$, then set the spline function $s(t)$ be a B-spline, $s = b$ and go back to Step 6.

Step 10: If $k \le S$ and the following equation holds $\sum_{t=1}^{N} \frac{[e_{k-1}(t) - e_k(t)]}{e_k{}^2(t)} > a$ then set $k = k + 1$, $s = 3$, and go back to Step 6. or set $e_{i+1,k+1}(t) = e(t)$ otherwise.

Step 11: Get the *ith* intrinsic mode function component $f_{i+1}(t) = e_{i+1,k+1}(t)$, and set $r_{i+1}(t) = r_i(t) - f_{i+1}(t)$;

Step 12: If the residue $r_{i+1}(t)$ is not a monotonic function, then set $i = i+1$, and go back to Step 5.

Step 13: If $p = 1$, let $g_{i,p}(t) = f_i(t)$ and $r_{m,p}(t) = r_{i+1}(t)$, attain the feature function set $g_p(t) = \{g_{1,p}(t), g_{2,p}(t), ...\}$, let $r_0(t) = \tilde{y}_{np}(t)$, $p = 2$, and go back to Step 4.

Step 14: Let $h_{i,np}(t) = f_i(t)$ and $s_{m,np}(t) = r_{i+1}(t)$, attain the feature function set $h_{np}(t) = \{h_{1,np}(t), h_{2,np}(t), ...\}$.

Step 15: Perform the feature extraction for $\tilde{y}_p$ and $\tilde{y}_{np}$ according to $g_p(t)$ and $h_{np}(t)$.

Step 16: Filter the features attained via $g_p(t)$ and $h_{np}(t)$, find out anomalous traffic components, and save resulting detection results into the file.

Simulation Result and Analysis

Now we deploy some tests to validate our detection approach for network traffic. In our simulation experimentations, we inject anomalous network traffic into normal background network traffic at four different time slots of 300, 700, 1100, and 1500 with the duration of 80, respectively. To avoid the random errors, we run 50 times simulation to attain the average detection results. The detection threshold is decided automatically according to our detection algorithm. In the following, for our algorithm, we analyze the feature extraction ability based on the principal component decomposition, the feature extraction ability based on the empirical mode decomposition, and anomaly detection ability. We use the real data from the Abilene backbone network to perform the simulation process. In our experiment, we select 1936 traffic value as our simulation data. In this case, we can construct a 44×44 traffic matrix to carry out the principal component decomposition process. The maximum iterative step number is set as 100, and all simulations are performed in the same setting.

Fig. 1 shows network traffic and principal component decomposition results, in which Fig. 1(a) and (b) denote the normal and abnormal network traffic, respectively, while Fig. 1(c) and (d) describe the principal and non-principal components extracted from abnormal network traffic in Fig. 1(b). Fig. 1(a) and (b) indicate that normal and abnormal traffic have no distinct difference, which leads to the larger challenge for anomaly detection ability of algorithms. Fig. 1(c) and (d) state that the principal features and secondary features of abnormal network traffic can be correctly extracted via our algorithm. It is clear that the principal component traffic reflects the principal characteristics of network traffic. This indicates that our algorithm is effective.

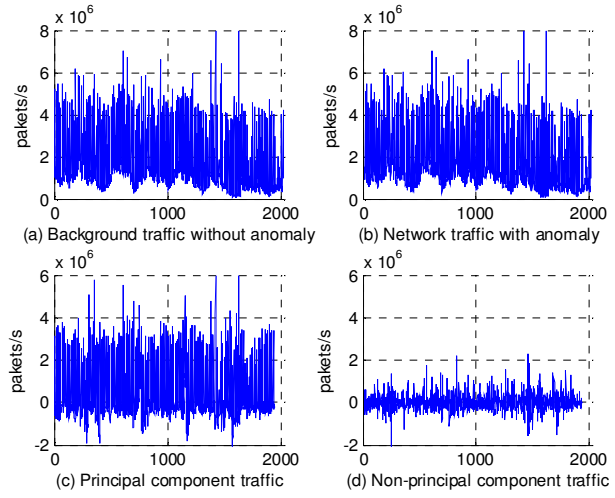

Figure 1. Network traffic and principal component traffic.

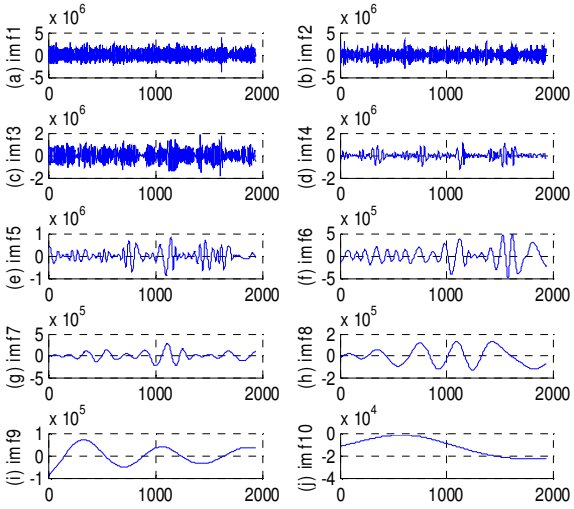

Figure 2. Empirical mode decompositions for principal component traffic.

Fig.2 plots the empirical mode decompositions for principal component traffic. From Fig. 2, we can clearly see that the principal component traffic can be characterized by 10 empirical mode functions accurately. It is very clear that the different empirical mode functions can capture the different features of the principal component traffic. Similarly, in Fig. 3, we plot the empirical mode decompositions for non-principal component traffic. From Fig. 3, we can also clearly see that the non-principal component traffic can be described by 10 empirical mode functions accurately. As shown in Fig. 2, it is very clear that the different empirical mode functions can capture the different features of the non-principal component traffic. This also states that our algorithm is promising.

Fig. 4 shows the traffic anomaly detection results via our algorithm, where the decided detection threshold is 0.3 and the dot-ling pulse curve denotes the time slots at which the anomalous traffic is injected. It is very interesting that the detection curve can effectively and accurately highlights the time slots at which anomalous network traffic happens. In such a case, we use the detection threshold to be able to correctly find out the abnormal and anomalous network traffic. Consequently, we can perform the accurate anomaly detection for network traffic. This further demonstrates that our algorithm can effectively find out the anomalous traffic.

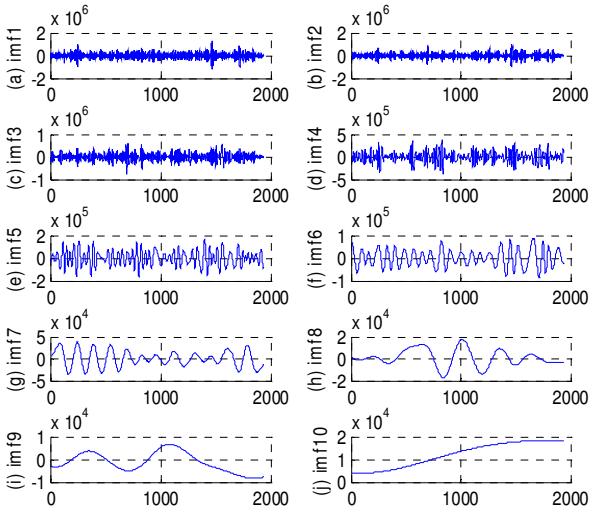

Figure 3. Empirical mode decompositions for non-principal component traffic.

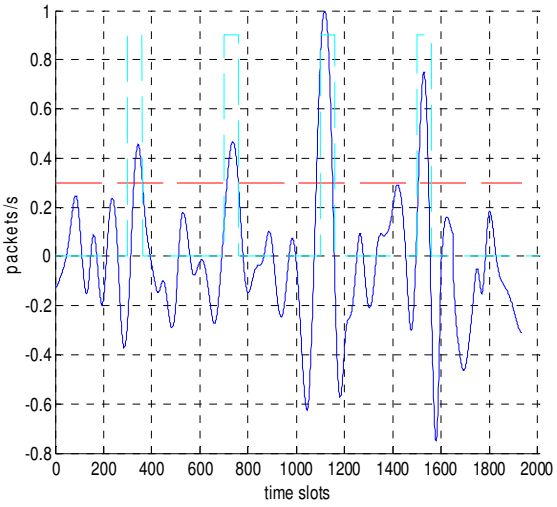

Figure 4. Traffic anomaly detection results.

Summary

This paper proposes a new quick detection approach to detect the anomaly components in network traffic, which combines the principal component analysis with the empirical mode decomposition method. Through converting network traffic series into a traffic matrix, the principal component decomposition is performed for the matrix. Accordingly, the principal and non-principal components of network traffic are attained. We use principal components to denotes the principal features in network traffic while non-principal components to describe the secondary features in network traffic. The empirical mode decomposition is used to decompose these two components. Then the different empirical mode functions are constructed to capture and characterize them, respectively. Finally, a quick anomaly detection algorithm is presented to perform the accurate recognition of anomalous network traffic. Simulation results show that our approach is promising.

References

[1] D. Jiang, Z. Xu, P. Zhang, et al., A transform domain-based anomaly detection approach to network-wide traffic, Journal of Network and Computer Applications, 2014, 40(2): 292-306.

[2] Y. Xiang, K. Li, W. Zhou, Low-rate DDoS attacks detection and trace back by using new information metrics, IEEE Transactions on Information Forensics and Security, 2011, 6(2): 426-437.

[3] Z. Yuan, D. Jiang, Q. Tang, et al., A time-frequency analysis-based detection algorithm for network traffic anomaly, in Proc. COIN'13, 2013, pp. 1-4.

[4] W. Xiong, H. Hu, N. Xiong, et al., Anomaly secure detection methods by analyzing dynamic characteristics of the network traffic in cloud communications, Information Sciences, 2014, 258(2014): 403-415.

[5] D. Jiang, C. Yao, Z. Xu, et al., Multi-scale anomaly detection for high-speed network traffic, Transactions on Emerging Telecommunications Technologies, 2015, 26(3): 308-317.

[6] T. Akgül, S. Baykut, M. E. Kantarci, et al., Periodicity-based anomalies in self-similar network traffic flow measurements, IEEE Transactions on Instrumentation and Measurement, 2011, 60(4): 1358-1366.

[7] D. Jiang, Z. Yuan, P. Zhang, et al., A traffic anomaly detection approach in communication networks for applications of multimedia medical devices, Multimedia Tools and Applications, 2016, online available, pp. 1-25.

[8] G. Thatte, U. Mitra, J. Heidemann, Parametric methods for anomaly detection in aggregate traffic, IEEE Transactions on Networking, 2011, 19(2): 512-525.

[9] D. Jiang, W. Qin, L. Nie, et al., Time-frequency detection algorithm of network traffic anomalies, in Proc. ICIIM'12, 2012, pp. 1-4.

[10] G. Thatte, U. Mitra, and J. Heidemann, Parametric methods for anomaly detection in aggregate traffic, IEEE/ACM Transactions on Networking, vol. 19, no. 2, pp. 512-525, 2011.

[11] B. Eriksson, P. Barford, R. Bowden, et al., Basisdetect: A model-based network event detection framework, in Proc. IMC, pp. 451-464, 2010.

[12] D. Jiang, C. Yao, W. Zhang, et al., A detection algorithm to anomaly network traffic based on spectral kurtosis analysis, in Proc. ITSim'13, 2013, pp. 980-983.

[13] P. Tune, D. Veitch, Sampling vs sketching: An information theoretic comparison, in Proc. of INFOCOM, 2011, pp: 2105-2113.