Abstract

The aim of this research is to analyze aggregate network traffic for anomaly detection. The accurate and rapid detection of network traffic anomaly is crucial to enhance the effective operation of a network. It is often difficult to detect the time when the faults occur in a network. In this paper, a new algorithm is presented to monitor the aggregate network traffic to rapidly detect the time anomaly occurs in a network. This is accomplished by monitoring the statistical characteristics of the time series representing the network behavior. The technique analyzes the network behavior using fractal dimension and discrete stationary wavelet transform. In the proposed method, after applying discrete stationary wavelet transform on the signal representing the network traffic, the fractal dimension of the decomposed signal is calculated in a sliding window. Then, variations of signal fractal dimension are considered for anomaly detection. Performance of the proposed method is compared with that of three other existing methods using both synthetic signal and real data. The results indicate superiority of the proposed technique in terms of accuracy compared to existing methods.
Designing an Approach for Network Traffic Anomaly Detection


Index Terms

Computer Science       Network Security

Keywords

anomaly detection   effective operation of the network   fractal dimension   wavelet transform