ABSTRACT

Increasing demands of users and internet services that occur at this time causes increasingly complex network infrastructure as well as more possible congested traffic on the network. It has an impact on the possibility of a system or network failure, and a decrease in QoS and the performance of a network, such as the occurrence of transient congestion on the network, which can cause many data packets to be dropped. To overcome this problem, the detection of anomalies on network traffic monitoring was carried out by utilizing the sparsity of the anomaly traffic matrix and low-rank property of the nominal traffic matrix, using the Batch Block Coordinate Descent (BCD) algorithm. Another important issue is the level of anomalies that occur on a network. Follow-up to overcome the anomalies in the network, it will be more optimal if the severity is known. The advantage obtained by knowing the level of the anomaly is that it can prioritize anomalies that must be addressed first, so that losses due to anomalies can be avoided. Then, after the estimated anomaly is obtained, $\hat{A}$, anomaly level classification was carried out. The level of the anomaly is divided into normal, low, medium and high levels. Because there is no reference in determining the threshold level anomaly and the anomaly data distribution is unknown, anomaly value constant is used as input to generate data. In the process of determining the algorithm for classification of anomalies, the threshold-1 (low), τ_1, is fixed based on the probability of false alarm, P_{FA} = 0.05. Then, threshold-2 (medium), τ_2, and threshold-3 (high), τ_3 are determined based on brute-force or exhausted search, by trying to shift the data sequences one by one to get the threshold with the most optimal accuracy. Performance tests with synthetic network data corroborate the effectiveness of the proposed algorithms and their accuracy for anomaly level classification.

Keywords: *Anomaly Detection*, *Congestion*, *Sparse*, *Low-Rank*.