Anomaly detection in BGP using machine-learning algorithms

Prerna Batta[a]

[a] *Simon Fraser University, Burnaby, BC, Canada*

Keywords:

1. Introduction

Border Gateway Protocol (BGP) anomalies often occur and techniques for their detection have recently gained visible attention and importance. The detection of BGP anomalies effects network performance. Hence, implementation of anomaly detection algorithms is important for improving the performance of routing protocols.

2. Aim

To detect anomalies in Border Gateway Protocol using machine learning algorithms.

3. Material and methods

A Matlab tool was created to detect anomalies in BGP using various machine learning algorithms. We extracted 37 BGP features in order to achieve reliable classification results. These features are sampled every minute during a five-day period, producing 7,200 samples for each anomaly event. They are used as inputs for classification models. The samples from two days before and after each anomaly event are considered to be regular test datasets and the third day was the peak of each anomaly event. We analyze performance of BGP anomaly detection models based on SVM, HMM, naive Bayes, Decision Tree, and ELM classifiers. The algorithms are tested using Internet traffic traces. The performance of these algorithms depends on the selected features and their combinations. The proposed algorithms are used to maximize the accuracy of detecting BGP anomalies and also compared based on accuracy and F-score.

4. Results

When the testing accuracy of the classifiers is low, feature selection is used to improve their performance. Performance of the classifiers is greatly influenced by the employed datasets.

5. Conclusions

Detecting network anomalies and intrusions are crucial in fighting cyber attacks and insuring cyber security to service providers and network customers. Machine learning techniques are one of the most promising approaches for detecting network anomalies and have been employed in analyzing BGP behavior.

6. Keywords

Boarder Gateway Protocol, feature extraction, feature selection, machine learning techniques.