International Conference on
Theoretical and Applied Computer Science and Engineering
(ICTACSE, 2017)
Ankara, Turkey, November 10-11, 2017

Application of Supervised Machine Learning in BGP Anomaly Detection

Marijana Ćosović[1] and Slobodan Obradović[1]
1 Faculty of Electrical Engineering, University of East Sarajevo, East Sarajevo, Bosnia and Herzegovina
marijana@etf.unssa.rs.ba, slobo.obradovic@gmail.com

The application of machine learning is on the rise and aimed at recognition and early detection of anomalies, both in the research community and in the industry. Since the Internet is not a centralized system and is made up of a multitude of autonomous systems, its proper functioning ie the connection of its parts, is based on the proper functioning of the BGP (*Border Gateway Protocol*) on the border gateway routers. The BGP protocol is the standard routing protocol on the Internet and is based on a trust model. As such it is targeted for attacks and harmful effects of anomalies.

One of the techniques of machine learning for anomaly detection is classification, which belongs to supervised learning and deals with classifying of data into a definite, finite number of classes. Machine learning models for detection of anomalies in BGP protocol are considered in this study: an anomaly either exists or does not exist. Support Vector Machines (SVM), Naïve Bayes (NB), decision tree, neural networks, ensemble methods were used to develop different models based on machine learning algorithms for better anomaly prediction.

We used various machine learning algorithms to improve BGP detection models performance measures. Specific scenarios of different types of anomalies affecting the BGP protocol are considered. We concluded that performance of the models used for classification depends on anomaly datasets used hence no single model performs the best on all considered datasets. Preprocessing of the datasets was beneficial in terms of improving performance measures as well as creating complex models such as filter and wrapper models.

Keywords: Machine learning, anomaly detection, BGP, supervised learning, classification

REFERENCES

[1] Marijana Ćosović, Slobodan Obradović, "BGP anomaly detection with balanced datasets," Tehnički vjesnik/Technical Gazette, vol. 25, no. 3, in press, June 2018.

[2] Marijana Ćosović, Slobodan Obradović, and Emina Junuz, "Deep learning for detection of BGP anomalies," in Proc. of Int. work-conf. on Time Series, Granada, Spain, Sept. 2017, vol. 1, pp. 487-498.

[3] Marijana Ćosović, Slobodan Obradović, "Ensemble methods for classifying BGP anomalies," Industrial Technologies, ISSN: 13149911, vol. 4, no. 1, pp. 12–20, June 2017.