Enhancement Method of Network Traffic Anomaly Detection Model Based on Adversarial Training With Category Tags

Authors : Zhang Shuqi, Liu Dan

Abstract : For the problems in intelligent network anomaly traffic detection models, such as low detection accuracy caused by the lack of training samples, poor effect with small sample attack detection, a classification model enhancement method, F-ACGAN(Flow Auxiliary Classifier Generative Adversarial Network) which introduces generative adversarial network and adversarial training, is proposed to solve these problems. Generating adversarial data with category labels could enhance the training effect and improve classification accuracy and model robustness. FACGAN consists of three steps: feature preprocess, which includes data type conversion, dimensionality reduction and normalization, etc.; A generative adversarial network model with feature learning ability is designed, and the sample generation effect of the model is improved through adversarial iterations between generator and discriminator. The adversarial disturbance factor of the gradient direction of the classification model is added to improve the diversity and antagonism of generated data and to promote the model to learn from adversarial classification features. The experiment of constructing a classification model with the UNSW-NB15 dataset shows that with the enhancement of FACGAN on the basic model, the classification accuracy has improved by 8.09%, and the score of F1 has improved by 6.94%.

Keywords : data imbalance, GAN, ACGAN, anomaly detection, adversarial training, data augmentation
Conference Title : ICSP 2022 : International Conference on Signal Processing
Conference Location : London, United Kingdom
Conference Dates : November 18-19, 2022

Open Science Index, Electronics and Communication Engineering Vol:16, No:11, 2022 publications.waset.org/abstracts/156929.pdf