World Academy of Science, Engineering and Technology
International Journal of Electronics and Communication Engineering
Vol:16, No:11, 2022

mKDNAD: A Network Flow Anomaly Detection Method Based On Multi-teacher Knowledge Distillation

Authors : Yang Yang, Dan Liu

Abstract : Anomaly detection models for network flow based on machine learning have poor detection performance under extremely unbalanced training data conditions and also have slow detection speed and large resource consumption when deploying on network edge devices. Embedding multi-teacher knowledge distillation (mKD) in anomaly detection can transfer knowledge from multiple teacher models to a single model. Inspired by this, we proposed a state-of-the-art model, mKDNAD, to improve detection performance. mKDNAD mine and integrate the knowledge of one-dimensional sequence and two-dimensional image implicit in network flow to improve the detection accuracy of small sample classes. The multi-teacher knowledge distillation method guides the train of the student model, thus speeding up the model's detection speed and reducing the number of model parameters. Experiments in the CICIDS2017 dataset verify the improvements of our method in the detection speed and the detection accuracy in dealing with the small sample classes.

Keywords : network flow anomaly detection (NAD), multi-teacher knowledge distillation, machine learning, deep learning
Conference Title : ICSP 2022 : International Conference on Signal Processing
Conference Location : London, United Kingdom
Conference Dates : November 18-19, 2022