Network attack detection scheme based on variational quantum neural network

ABSTRACT

Network attack may have a serious impact on network security. With the rapid development of quantum machine learning, variational quantum neural network (VQNN) has demonstrated quantum advantages in classification problems. The intrusion detection system (IDS) based on quantum machine learning has higher accuracy and efficiency than the IDS based on traditional machine learning. In this work, we propose a intrusion detection scheme based on VQNN, which is composed of variational quantum circuit (VQC) and classical machine learning (ML) strategy. In order to verify the effectiveness of the scheme, we used the VQNN model and some classic ML models (Such as artificial neural network, support vector machines, K-Nearest Neighbors, Naive Bayes, decision tree) to conduct comparative experiments. The results indicate that the proposed IDS model based on VQNN has a 97.21% precision, which is higher than other classic IDS models. Furthermore, our VQC can be deployed on the overwhelming majority of recent noisy intermediate-scale quantum machines (such as IBM). This research will contribute to the construction of general variational quantum framework and experimental design and highlight the potential hopes and challenges of hybrid quantum classical learning schemes.