Quantum Anomaly Detection Frameworks for Network Security

Moe Hdaib, Sutharshan Rajasegarar, and Lei Pan

The increasing frequency and sophistication of cyber security incidents necessitate robust and efficient methods to identify and mitigate anomalous activities within network traffic. Traditional machine learning and deep learning techniques have been extensively researched for anomaly detection. However, leveraging the computational power of quantum deep learning to process complex feature correlations for anomaly detection remains relatively unexplored. This paper addresses this gap by investigating quantum machine learning (QML) and quantum deep learning (QDL) methodologies to enhance the accuracy of network attack detection. Given the critical nature of network security in safeguarding sensitive information and maintaining operational integrity, the proposed quantum-based approaches aim to significantly improve anomaly detection capabilities.

Quantum machine learning holds great promise for various applications due to its unique attributes, such as parallelism and the ability to process vast amounts of data simultaneously. Recent advancements in QML have shown its potential in accelerating processing speeds and addressing data dimensionality issues, making it a suitable candidate for anomaly detection tasks. Notably, quantum autoencoders (QAEs) have been successfully applied to complex quantum systems and other areas like communication and distributed computation. Integrating QAEs with quantum machine learning algorithms can provide a powerful framework for detecting anomalies in network traffic, offering significant improvements over classical methods.

In this paper, we analyse our three-novel quantum autoencoder-based frameworks for anomaly detection in network traffic [1]. These frameworks integrate quantum autoencoders with quantum one-class support vector machines, quantum random forests, and quantum k-nearest neighbor, respectively. By combining the strengths of quantum computing and deep learning, the proposed hybrid models aim to efficiently identify anomalies in network flows from both computer and Internet of Things (IoT) networks. The integration of quantum autoencoders enables effective dimensionality reduction, improving the detection accuracy and training speed of the anomaly detection models. The implementation leverages parameterized quantum circuits and deep neural networks to process and analyze network traffic data.

The evaluation of the proposed frameworks is conducted using benchmark datasets, including KDD99, IoT-23, and CIC IoT 23, which comprise various network traffic scenarios and attack types. The results demonstrate that all three quantum frameworks exhibit high potential in accurately detecting network traffic anomalies. Among the three, the framework combining quantum autoencoder with quantum k-nearest neighbor achieves the highest accuracy, showcasing the effectiveness of this hybrid approach. Furthermore, all our proposed quantum frameworks outperform their classical counterparts. These findings underscore the relevance and promising potential of developing quantum frameworks for anomaly detection, paving the way for future advancements in network security. The successful application of these quantum-based methodologies highlights their significance in addressing the evolving challenges of cyber security.

References

[1] Hdaib, M., Rajasegarar, S. & Pan, L. Quantum deep learning-based anomaly detection for enhanced network security. Quantum Mach. Intell. 6, 26 (2024). https://doi.org/10.1007/s42484-024-00163-2