Machine Learning-Based Anomaly Detection in NFV: A Comprehensive Survey

ABSTRACT

Network function virtualization (NFV) is a rapidly growing technology that enables the virtualization of traditional network hardware components, offering benefits such as cost reduction, increased flexibility, and efficient resource utilization. Moreover, NFV plays a crucial role in sensor and IoT networks by ensuring optimal resource usage and effective network management. However, adopting NFV in these networks also brings security challenges that must promptly and effectively address. This survey paper focuses on exploring the security challenges associated with NFV. It proposes the utilization of anomaly detection techniques as a means to mitigate the potential risks of cyber attacks. The research evaluates the strengths and weaknesses of various machine learningbased algorithms for detecting network-based anomalies in NFV networks. By providing insights into the most efficient algorithm for timely and effective anomaly detection in NFV networks, this study aims to assist network administrators and security professionals in enhancing the security of NFV deployments, thus safeguarding the integrity and performance of sensors and IoT systems.