English Abstract-Eslam Farsimadan

The Internet and advanced communication networks, such as IoT and cellular networks, produce enormous and diverse traffic data flows. The behavior of network traffic in these networks is highly intricate due to factors like device mobility and network heterogeneity. As a result, conventional network security and management methods struggle to handle the challenges of securing, monitoring, and analyzing the network and data. These challenges include issues such as the efficacy of classification and detection strategies, precision, accuracy, and the ability to process big data in real-time.

Recently, machine learning and deep learning have proven to be highly effective in addressing network security concerns and have demonstrated superiority over traditional methods. Consequently, researchers in the field of networking are turning to these machine learning and deep learning models for network security and management.

Motivated by the success and effectiveness of these models, this thesis concentrates on addressing two crucial and challenging issues in network security through dynamic analysis, machine learning, and deep learning models, with a particular emphasis on artificial neural networks. More precisely, it presents new learning-based techniques for attack classification and malware detection.

First, a general introduction with some motivations for this thesis is presented. Then, the state-of-the-art is investigated, and the most effective artificial intelligence-based methods related to the above mentioned network security aspects are reported. After that, the primary materials and preliminaries for constructing the proposed models, such as neural network types, recurrence plots, and so on, are introduced in detail. Finally, the proposed methods for attack classification and malware detection are investigated in terms of mathematical background, model architecture, experimental setting, and evaluation.

Moreover, the proposed methods are analyzed from a theoretical perspective and through specific performance evaluation experiments on real network traffic datasets. The obtained results, in the presence of several unbalanced datasets instances, prove the effectiveness of the proposed approaches.

Keywords: Network Security, Attack Detection, Attack Classification, Malware Detection, Machine Learning, Deep Learning, Neural Networks, Recurrence Plots, Markov Chain.