Study of Effective Framework Combining Sparse Autoencoder Based Feature Transfer Learning and Long Short-Term Memory for Network Intrusion Detection System

Zolzaya Kherlenchimeg

In recent years, a deep neural network has been solving a variety of complex problems of science and engineering fields ranging from healthcare to transportation. Among them, one of the most crucial issues is to protect a network against cyber threats. To address the issue, we design to create an effective novel framework for intrusion detection system (IDS). The purpose of this graduation thesis is to investigate the effect if a two-stage IDS framework based on a single-layer Sparse Autoencoder (SAE) and Long Short-Term Memory (LSTM). Initially, the single-layer SAE learns new feature representations of the data through the nonlinear mapping, following that, the new feature representations are fed into the LSTM model to classify network traffic whether it is being normal or attack. The proposed framework was evaluated on the benchmark NSL-KDD dataset, where the mean accuracy of the proposed method was achieved 84.8%. The experimental results show that the two-stage IDS framework achieved better classification accuracy than the existing state-of-the-art methods.

Chapter 1 presents the vulnerabilities of cyber infrastructure and conventional techniques for cyber defense. We discuss an effective methodology that uses advanced machine learning methods to build an intrusion detection system (IDS) which plays a vital role in detecting cyber-attack. Then, we present the main objectives of the thesis and a brief description of the problem statement and contributions.

Chapter 2 introduces the fundamental knowledge, key issues and challenges in IDS. Furthermore, we review the pieces of literature that address cyber security issues using machine

learning and deep learning techniques on a benchmark NSL-KDD dataset, including anomaly detection, feature learning and feature selection of attacks patterns.

Chapter 3 provides a detailed overview of a network intrusion detection system. Then provides a comprehensive discussion on deep learning approaches that we used to build the proposed framework.

Chapter 4 introduces the first attempt to design a deep learning approach that combined sparse autoencoder with recurrent neural networks for the intrusion detection system. We evaluate the performance of the proposed method on the NSL-KDD dataset. We conclude the limitations of using the proposed approach.

Chapter 5 demonstrates a more effective framework combining the SAE based feature transfer learning and LSTM for NIDS. We evaluate the performance of the proposed framework on the NSL-KDD dataset in two scenarios. Consequently, the results of the proposed framework compared with the results of similar prior studies.

Chapter 6 concludes the development of the proposed framework and their results; as well as insights to overcome the limitations of our work along with the enhancements.