**Abstract**

Intrusion detection has attracted a considerable interest from researchers and industries. The community, after many years of research, still faces the problem of building reliable and efficient IDS that are capable of handling large quantities of data, with changing patterns in real time situations. The work presented in this manuscript classifies intrusion detection systems (IDS). Moreover, a taxonomy and survey of shallow and deep networks intrusion detection systems is presented based on previous and current works. This taxonomy and survey reviews machine learning techniques and their performance in detecting anomalies. Feature selection which influences the effectiveness of machine learning (ML) IDS is discussed to explain the role of feature selection in the classification and training phase of ML IDS.. Deep learning, as one of the most currently remarkable machine learning techniques, has achieved great success in many applications such as image analysis, speech recognition and text understanding. It uses supervised and unsupervised strategies to learn multi-level representations and features in hierarchical architectures for the tasks of classification and pattern recognition. In this paper, we review the emerging researches of deep learning models for NIDS feature learning. Furthermore, we point out the remaining challenges of Intrusion detection system deep learning and discuss the future topics.