**ABSTRACT**

To secure a network from intrusion and for the conﬁdentiality of any data, an Intrusion Detection System plays a vital role. The main objective is to achieve an accurate performance of an NIDS system which adepts in detection of various types of attacks in the network. In this report, we have explored the performance of an Network Intrusion Detection System (NIDS) which can detect attacks in the network using Deep Reinforcement Learning Algorithm (DRL). We have exploited Deep Q Network algorithm which is a value-based Reinforcement Learning algorithm technique used in detection of network intrusions. Moreover, we have analysed the accuracy of our model in comparison with diﬀerent types of models. In this paper, we illustrated the comparison of our NIDSDQN model to a previous model designed in other approaches like J48, artiﬁcial neural network, random forest, support vector machine. Our Goal is to detect attacks without depending on the past experience and at its ﬁrst attempt. We used data set for minimising the false alarm rate. Previous work was based on a benchmark dataset such as KDD-99, NSL-KDD, which shares the same attributes for all models. We have worked on similar type of dataset which aided as an eﬀective means in detection of diﬀerent types of attacks. The Deep Q Network-Intrusion Detection System (DQN-IDS) model improves the accuracy and performance an IDS and provides a new means as a research method for intrusion detection.

Keywords: Network Security, Machine Learning, Deep Q Network, Artificial Neural Network, DDoS, NIDS