Attack Detection in Software Defined Network using RNN

Problem Statement

Software defined Network is an emerging network architecture that is dynamic, programmable and adaptable which makes it ideal for high-bandwidth and dynamic nature of today's applications. It is a programmable network, but it is prone to different type of attacks due to its centralized architecture. Software Defined Networking Technology (SDN) detect and monitor network security problems because of its programmable network control features. In this work, we are going to use the Recurrent neural network (RNN) model for detection of the attacks into one of the four categories (Probe, DOS, R2L and U2R).

Background

Previously, several important work and investigations have been done in order to solve the DoS attack in SDN. Some have used entropy-based approaches, threshold-based approach. In this work we have try to explore the use of deep learning algorithm like RNN for detection of DoS attack. We have taken the publicly available dataset of NSL-KDD and KDD-cup99.

Methodology

Step 1: Dataset preparation This will involve pre-processing the data which involves removing the redundant values, filling the missing values, preparing the data so that Machine Learning algorithm can be applied. Step 2: Developing a machine learning model for attack detection. In this step a Recurrent neural network model for intrusion detection is developed. Step 3: Training and experimentation on datasets Training and testing is performed on RNN model on the created datasets to do the prediction accurately. Step 4: Deployment and analysis on real life scenario: The trained and tested neural network model will be deployed in a real-life scenario for further analysis where attack detection will be leveraged

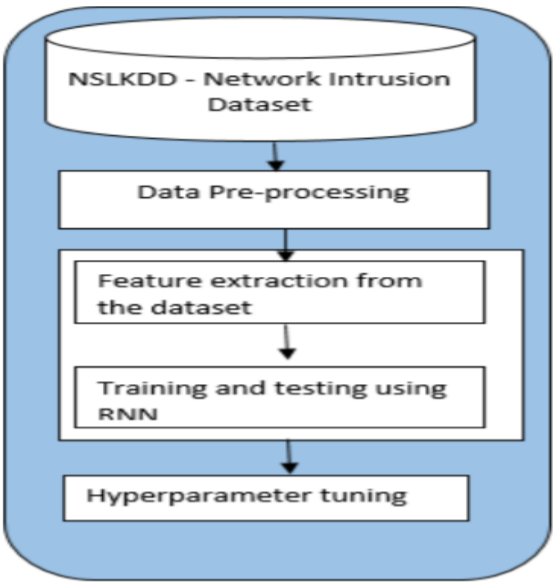

Figure 1 Block diagram of proposed methodology for Attack Detection.

Experimental Design Dataset: Publicly available dataset is used. NSL-KDD dataset contains the unique records from the complete KDD dataset. In total, there are 42 features of a flow and a label is assigned to each either as an attack type or as normal. The last feature contains data about the various categories of attacks. The various attack classes are DoS, Probe, R2L and U2R.

Software and Hardware Requirements Python based Machine Learning and Deep Learning libraries will be exploited for the development and experimentation of the project. Tools such as Anaconda Python, and libraries such as Tensorflow, and Keras will be utilized for this process.