# Network Behavior Analysis Techniques for Cyber-Attack Detection

Network behavior analysis is the technique to counter threats (Al-Mohannadi, 2016). By utilizing these techniques, we can detect any abnormal activity running through any network and after detecting such activities, it’ll give an automated response or it will inform the authorities about it. The network behavior analysis uses advanced artificial intelligence techniques and machine learning models to detect hidden threats and abnormal activities in those parts of the network where any other security tool can’t perform. We are connected to each other through internet, from online shopping to online banking we use internet, the users browsing internet can be the victims of cyber-attacks. (Raiyn, 2014) gave a wonderful comparison of different cyber-attacks that are happening these days which include Daniel of Service Attacks (DOS), R2L attacks, and U2R attacks, etc. (Raiyn, 2014) also discussed the cure to these threats and attacks. They discussed the Intrusion Detection System (IDS), Misuse detection of the network, Anomaly Detection system, etc.

The Intrusion Detection System (IDS) can be a physical device or a software program that is intelligent enough to monitor different networks and systems for abnormal activities, malicious threats, or terms and policies violation (Raiyn, 2014). These types of software are based on machine learning and artificial intelligence algorithms. These models are trained on the historical data which are put into production to detect malicious activities over networks.

There are many machines learning models which can be used in Intrusion Detection System (IDS), the problem in IDS is that we have to detect that either the activity is normal or abnormal based on different features. For this purpose, we have to train machine learning classifiers. We have a dataset that contains a variety of intrusions simulated over a military network. We will use different machine learning classification models and give the accuracy comparison at the end, the higher the accuracy, the best is the model for detecting any anomaly activity over the network. The purpose of doing so is because we will get the highest and more accurate model for final predictions. The workflow of the model training and testing is given below.

Classification

Select best model

Model building

We will use different models

EDA

Processing

Data

# References

Al-Mohannadi, H. M. (2016). Cyber-Attack Modeling Analysis Techniques: An Overview. *IEEE 4th international conference on future internet of things and cloud workshops*.

Raiyn, J. (2014). A survey of Cyber Attack Detection Strategies. *International Journal of Security and Its Applications*.