NETWORK INTRUDER DETECTION USING DEEP LEARNING

Introduction

In the modern era, Convolutional neural network (CNN) architectures in deep learning have achieved significant results in the field of computer vision. To transform this performance toward the task of intrusion detection (ID) in cyber security, this topic models network traffic as time-series, particularly transmission control protocol / internet protocol (TCP/IP) packets in a predefined time range with supervised learning methods such as multi-layer perceptron (MLP), CNN, CNN-recurrent neural network (CNN-RNN), CNN-long short-term memory (CNN-LSTM) and CNN-gated recurrent unit (GRU), using millions of known good and bad network connections. To measure the efficacy of these approaches we evaluate on the most important synthetic ID data set such as KDDCup 99. To select the optimal network architecture, comprehensive analysis of various MLP, CNN, CNN-RNN, CNN-LSTM and CNN-GRU with its topologies, network parameters and network structures is used. The models in each experiment are run up to 1000 epochs with learning rate in the range [0.01-05]. CNN and its variant architectures have significantly performed well in comparison to the classical machine learning classifiers. This is mainly due to the reason that CNN have capability to extract high level feature representations that represents the abstract form of low level feature sets of network traffic connections.

Recently, technology improvements have led to the faster information access over the internet. The ease of access of the data has also improved by the introduction of mobile computing platforms. The numbers of ecommerce companies are also increasing in the market. This has led to the increasing use of servers and sensitive information is transferred using the internet. This in turn has led to the increase in the threat from the attackers. Such cases increase the concern of developers and industry to develop measures to prevent such attacks. The attackers are using Virtual Private Networks (VPN) to mask the IP and MAC addresses during an attack on a network and thus keeping their identity hidden. Several types of network frauds have been carried out over the internet. Some of them include spams, website defacements , probing etc. A solution to this problem is to use the statistical parameters in the network to detect the intrusions caused. The suggested model would be controlling the traffic of network by curbing malicious efforts. It would seek for solving the issue of Spam, delay in response of server, illicit access to the network resources etc. This is applicable in many Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) . A parameter that could be affecting the process of the IDS is noise. The noise affecting the system could raise false alarms as

attacks. In the present day traffic scenario, some of the real attacks may get miss classified under the class of false alarm, increasing the False Alarm Rat.

The two types of the IDS systems are:

- Signature based IDS (S-IDS)
- Anomaly based IDS (A-IDS)

S-IDS is based on predefined parameter sets collected from previous attacks. On the other hand A-IDS analyses the network traffic and interprets the intruder. This is the most prevalent method used in the industry as it is dynamic and can be programmed to learn from the new attacks on a regular basis. The signature based IDS is not capable of detecting severe attacks on the system. IDS would be providing the information about the source of the sender. But fake IP would be received in the case where the packet is encapsulated or Virtual Private Network (VPN) is utilized. This work would attempt for solving few of the above stated issues. The issue is to identify any malicious type of activity or attack on the network utilizing anomaly dependent statistical methods, & relevant features selection depending on the acquired outcomes. The selection of features would be playing an important role in the elimination of irrelevant and redundant attributes, so that it would be choosing the relevant attributes to build the model.

Existing system

Network intrusion detection systems (NIDS) are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network. It performs an analysis of passing traffic on the entire subnet, and matches the traffic that is passed on the subnets to the library of known attacks. Once an attack is identified, or abnormal behaviour is sensed, the alert can be sent to the administrator. An example of an NIDS would be installing it on the subnet where firewalls are located in order to see if someone is trying to break into the firewall. Ideally one would scan all inbound and outbound traffic, however doing so might create a bottleneck that would impair the overall speed of the network. OPNET and NetSim are commonly used tools for simulating network intrusion detection systems. Waterfall for Intrusion Detection Systems (IDS) enables safe monitoring of OT networks. Waterfall for IDS unidirectional hardware emulates OT mirror & SPAN ports to network intrusion sensors on IT networks. With Waterfall for IDS in place, industrial enterprises can confidently host OT sensors on IT networks where the sensors are easily managed and updated by central SOC analysts, without risk to physical operations. Waterfall for IDS is a hardware-enforced, physical barrier that prevents remote attacks, malware, DOS attacks, ransomware and human errors originating on IT networks from compromising or impairing physical operations, while enabling seamless interoperability with intrusion detection system platforms.

But today, the intrusion detection schemes are rarely using deep learning techniques.

Proposed system

NIDS can be combined with other technologies to increase detection and prediction rates. Artificial Neural Network based IDS are capable of analysing huge volumes of data, in a smart way, due to the self-organizing structure that allows INS IDS to more efficiently recognize intrusion patterns. Neural networks assist IDS in predicting attacks by learning from mistakes; INN IDS help develop an early warning system, based on two layers. The first layer accepts single values, while the second layer takes the first's layers output as input; the cycle repeats and allows the system to automatically recognize new unforeseen patterns in the network.

Conclusion

An Intruder Detection System needs to detect anomalies in the network based on the input parameters.