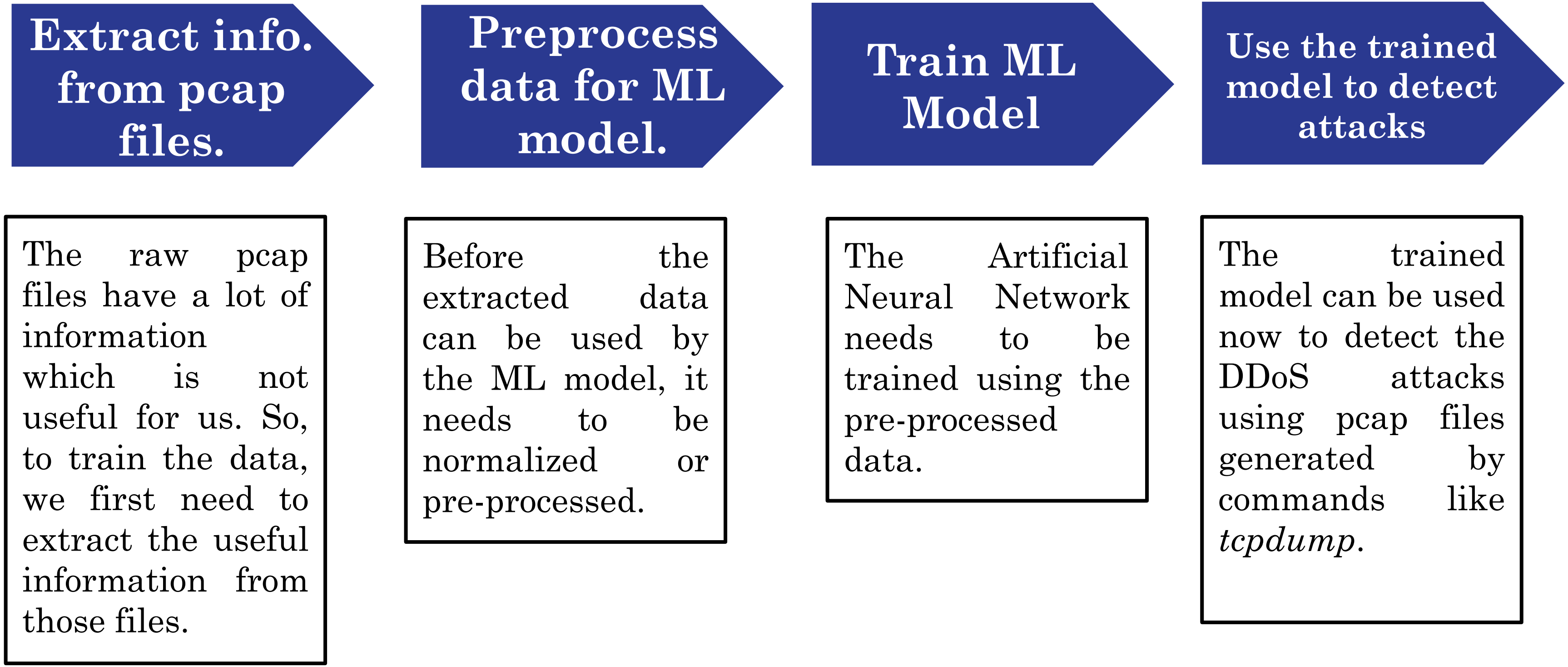
Detection of DDoS Attacks through Machine Learning

Team Members:
Rithik Sachdev
Shreya Mishra
Aarushi Ghadiya
Shekhar Sharma

Project Guides:

Prof. Vandan Tewari
Prof. Veerendra Shrivastav

Overall flow of information



Extract info. from pcap files.

The raw pcap files have a lot of information which is not useful for us. So, to train the data, we first need to extract the useful information from those files.

Preprocess data for ML model.

Before the extracted data can be used by the ML model, it needs to be normalized or pre-processed.

Train ML Model

The Artificial Neural Network needs to be trained using the pre-processed data.

Use the trained model to detect attacks

The trained model can be used now to detect the DDoS attacks using pcap files generated by commands like *tcpdump*.

Project Implementation

Code Files:

ANN.py

Contains the Artificial Neural Network Model for the detection of attacks.

DDoS_Detector.py

Main controlling program file which uses all the others to train and run the model.

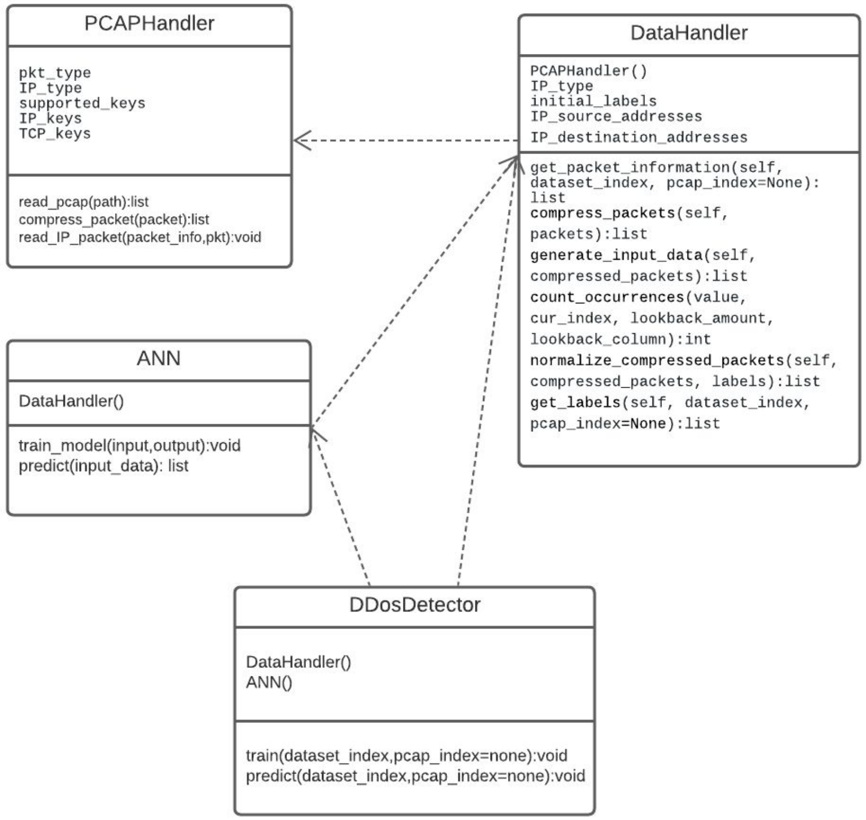
data_handler.py

Uses the data extracted from pcap_handler.py and generates input data for the ML model.

pcap_handler.py

Contains the code to read the pcap files and extract useful information from those files.

Class Diagram


PCAPHandler
pkt_type
IP_type
supported_keys
IP_keys
TCP_keys
read_pcap(path):list
compress_packet(packet):list
read_IP_packet(packet_info,pkt):void
DataHandler
PCAPHandler()
IP_type
initial_labels
IP_source_addresses
IP_destination_addresses
get_packet_information(self, dataset_index, pcap_index=None): list
compress_packets(self, packets):list
generate_input_data(self, compressed_packets):list
count_occurrences(value, cur_index, lookback_amount, lookback_column):int
normalize_compressed_packets(self, compressed_packets, labels):list
get_labels(self, dataset_index, pcap_index=None):list
ANN
DataHandler()
train_model(input,output):void
predict(input_data): list
DDosDetector
DataHandler()
ANN()
train(dataset_index,pcap_index=none):void
predict(dataset_index,pcap_index=none):void

Class Diagram

Code Explanation

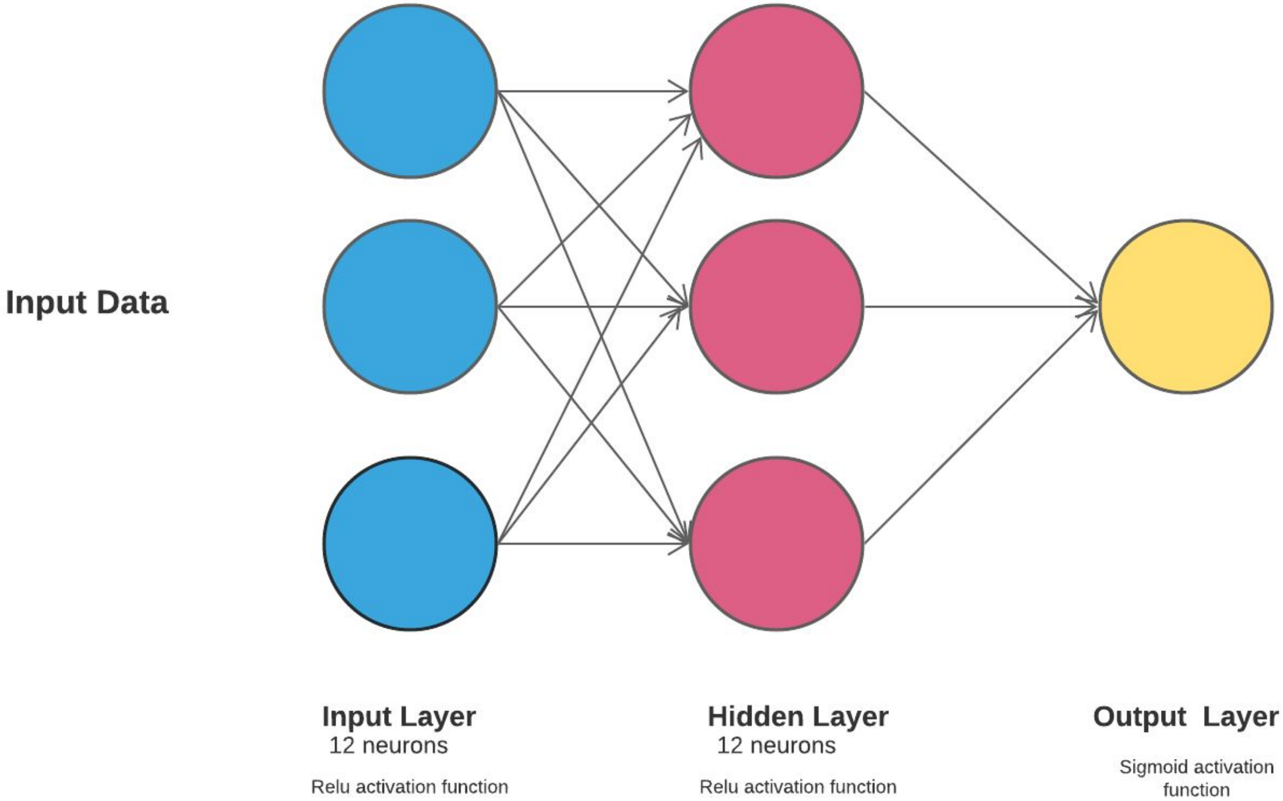
ANN.py
DDoS_Detector.py
Data_handler.py
pcap_handler.py

We will now switch to the code for better understanding.

https://github.com/rithiksachdev/DDoSAttackDetection

Scan the QR code for quick access

Artificial Neural Network



Input Data

Input Layer
12 neurons

Relu activation function

Hidden Layer
12 neurons

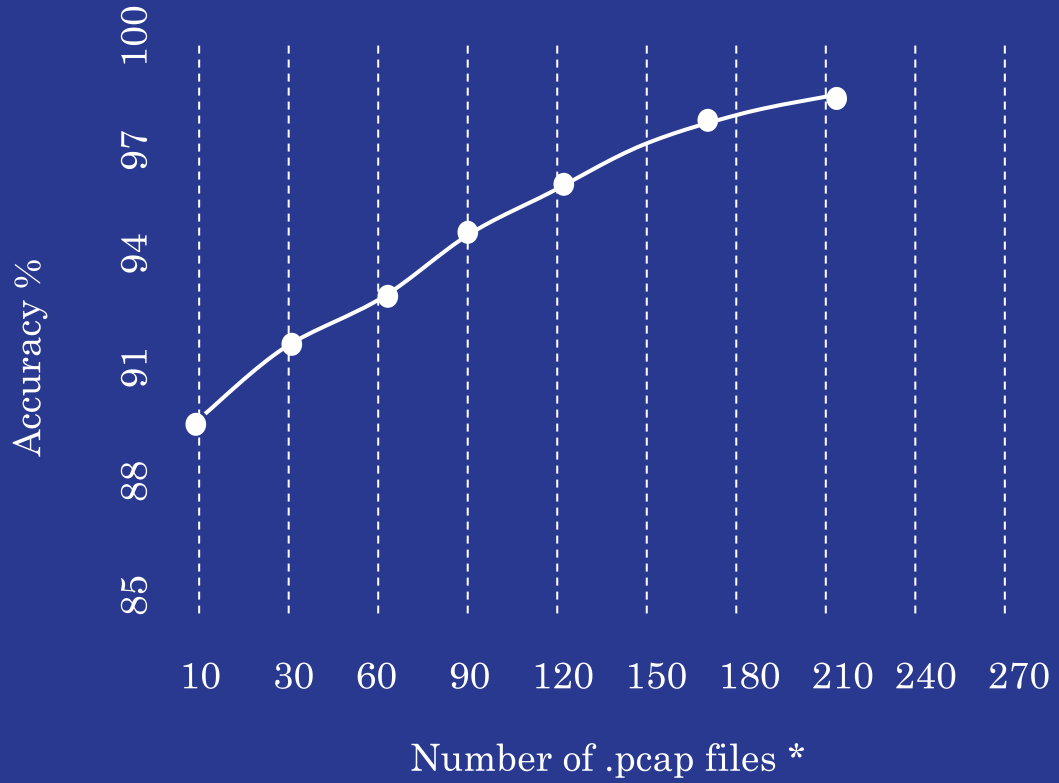
Relu activation function

Output Layer

Sigmoid activation function

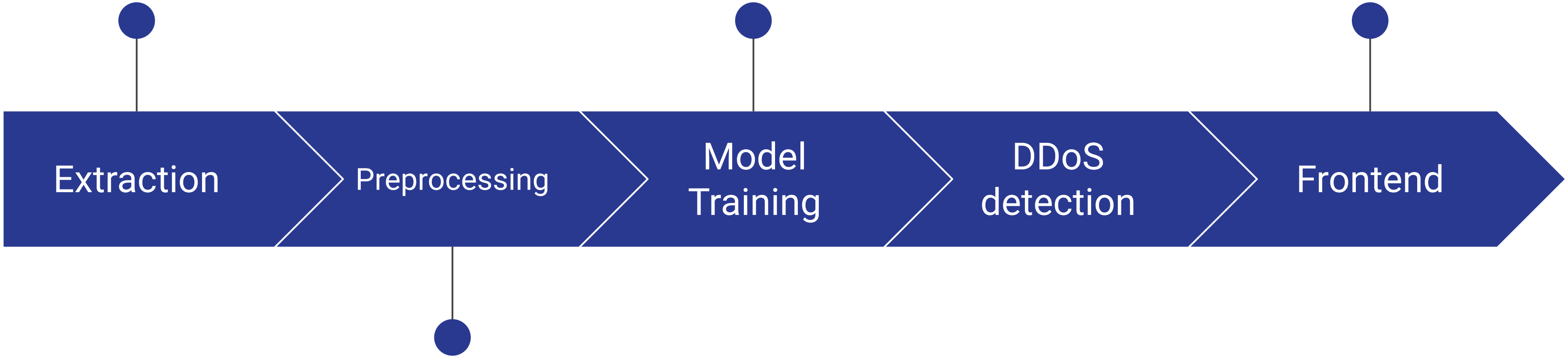
Artificial Neural Network

Results so far:



* *Each .pcap file contains 10,000 packets.*

Pending Work



Extraction

The data currently used is not sourced from live sniffing. Live sniffing feature will be added.

Preprocessing

Right now, we are only using basic parameters, we will increase that for feature selection.

Model Training

We are currently using only ANN, we will use other models also for comparison.

DDoS detection

Frontend

The whole system is currently on command line, a frontend will be added for ease of access.

Thank You