Robust and Secure Data Transmission Using Artificial Intelligence Techniques in Ad-Hoc Networks

Wireless networks are self-organizing which means they will discover neighbours to route data to destination by themselves and require no man power. This wireless devices runs on battery and cannot install heavy computation antivirus on this devices for network protection from attacks. Malicious users may take advantage of this and can execute various attacks such as DDOD attack, MITM attack, Black Hole Attack and many more on wireless devices. In Black hole attack malicious user may gain entry to wireless devices and then issue command to drop all packets.

To overcome from such attacks author of this paper employing Robust and secure data transmission using machine learning and Artificial Intelligence algorithms. This algorithms will inspect packets of wireless devices and if device contains malicious commands then it drop such packets and only accept non-attacks packets.

To improve attack detection rate author applying ABC (Artificial bee colony) algorithm to select important or relevant attributes from network packet and then apply SVM algorithm to get signatures and this signatures get trained with Artificial Neural Network algorithm to predict weather network packet contains normal signature or attack signature.

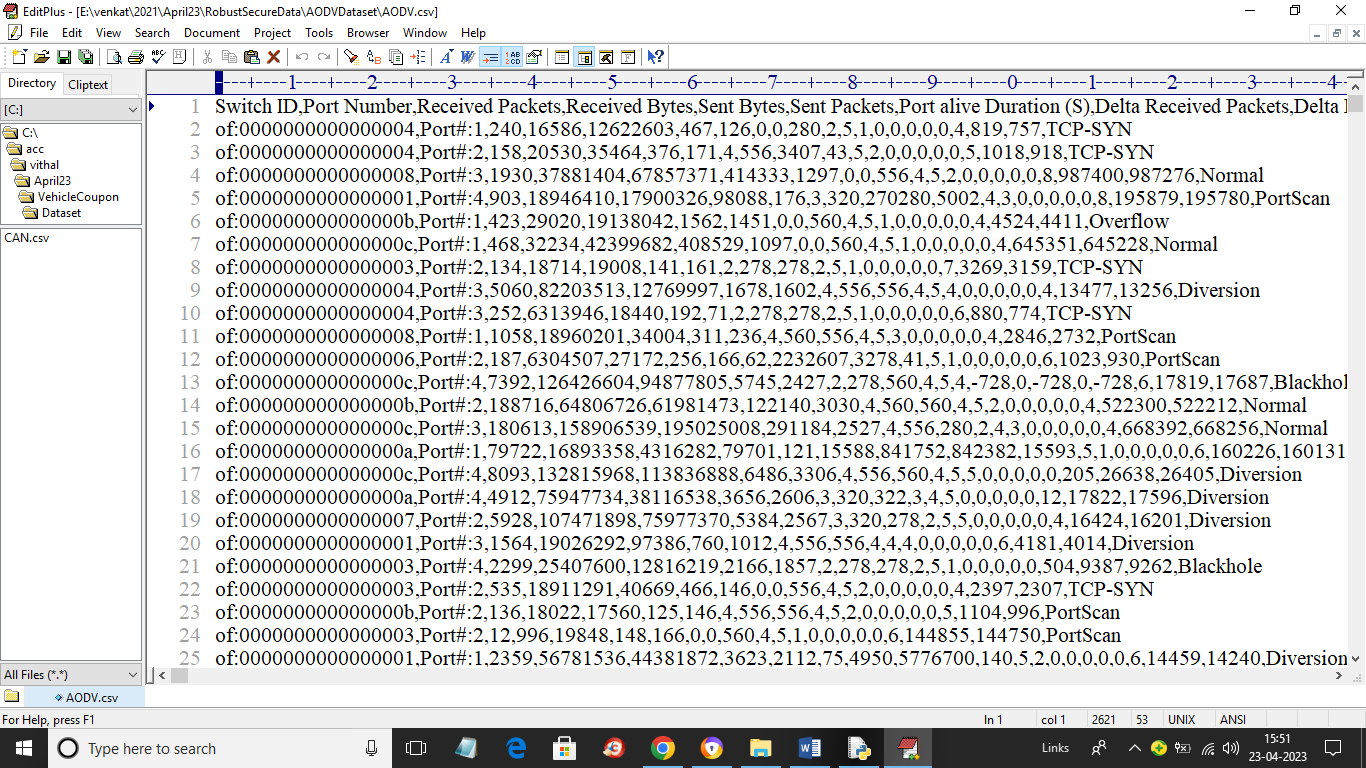
Author has evaluate algorithm performance in terms of Throughput, delay and PDR and if all attacks avoided then more packet will get transfer so throughput and PDR get increased and DELAY get decreased.

Author has compare propose ABC + SVM + ANN algorithm performance with Random Forest and Decision Tree and in all algorithm Propose is giving high throughput

To implement this project we have designed following modules

1. Upload AODV Dataset: using this module we will upload AODV dataset with normal and attack packets
2. Preprocess Dataset: using this module we will process dataset to remove missing values and then encode all non-numeric values into numeric values and then normalize dataset values
3. Run Propose ABC, SVM & ANN Model: processed data will be input to ABC algorithm to select important attributes and then input to SVM to get SVM predicted signatures and this signatures will be input to ANN model to predict normal or attack records and then calculate throughput, PDR and Delay based on predicted output
4. Run Random Forest Algorithm: using this module we will train Random Forest algorithm on processed data to predict attack and then calculate throughput, PDR and Delay based on predicted output
5. Run Decision Tree Algorithm: using this module we will train Decision Tree algorithm on processed data to predict attack and then calculate throughput, PDR and Delay based on predicted output
6. Comparison Graph: using this module we will plot throughput, delay and PDR graph between all algorithms
7. Attack Detection from Test Data: using this module we will upload test data and then algorithm will predict weather test data is normal or contains attack

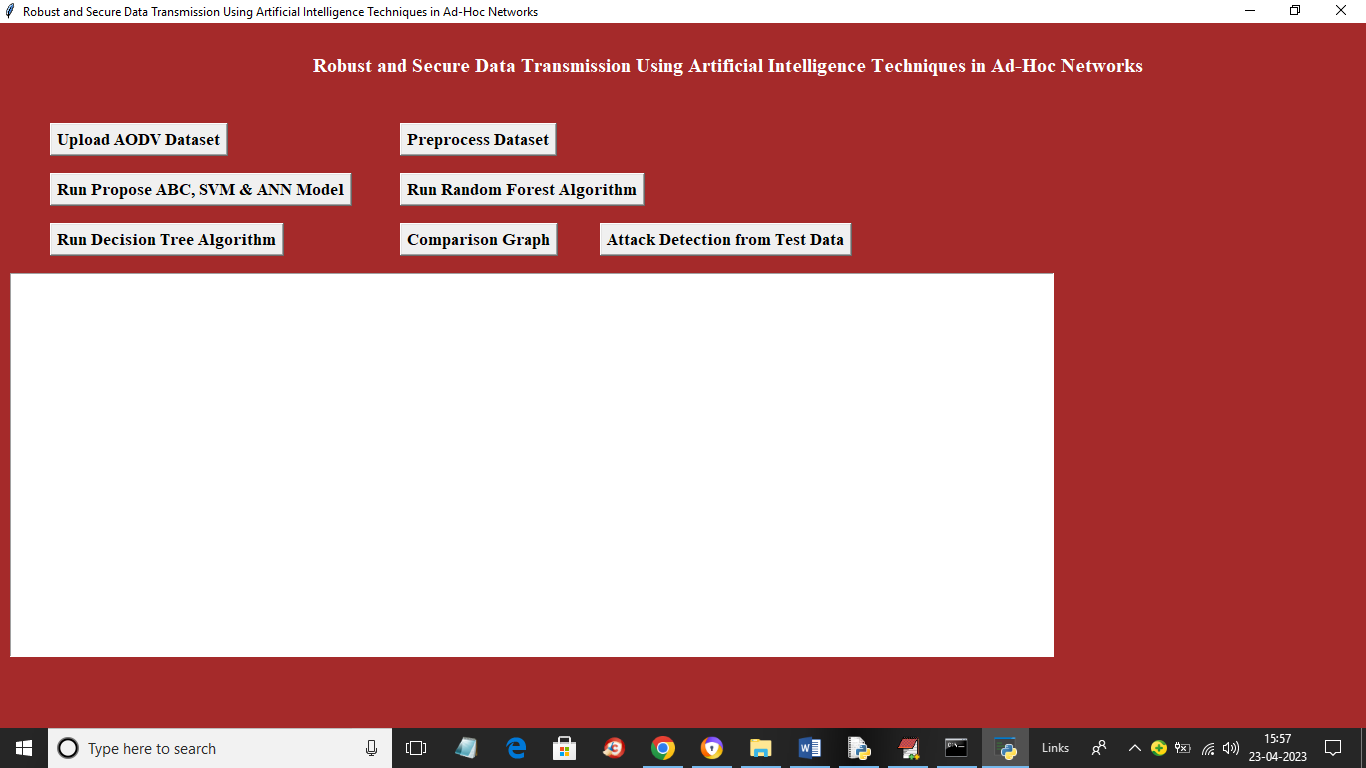
To train above algorithms we are using below AODV dataset



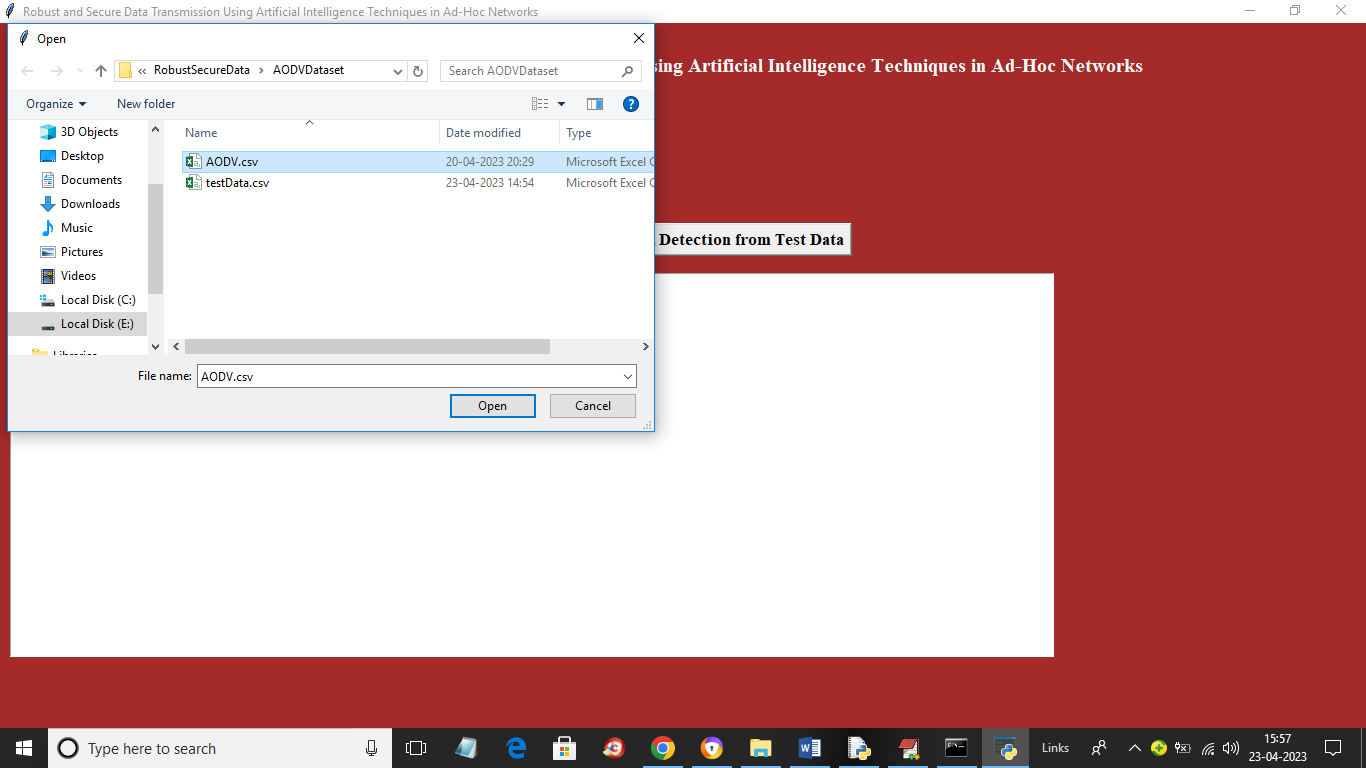
In above dataset screen first row represents dataset column names and remaining rows contains dataset values and in last column we have class labels Normal or attack names. So by using above dataset we will train and test all algorithms performance

SCREEN SHOTS

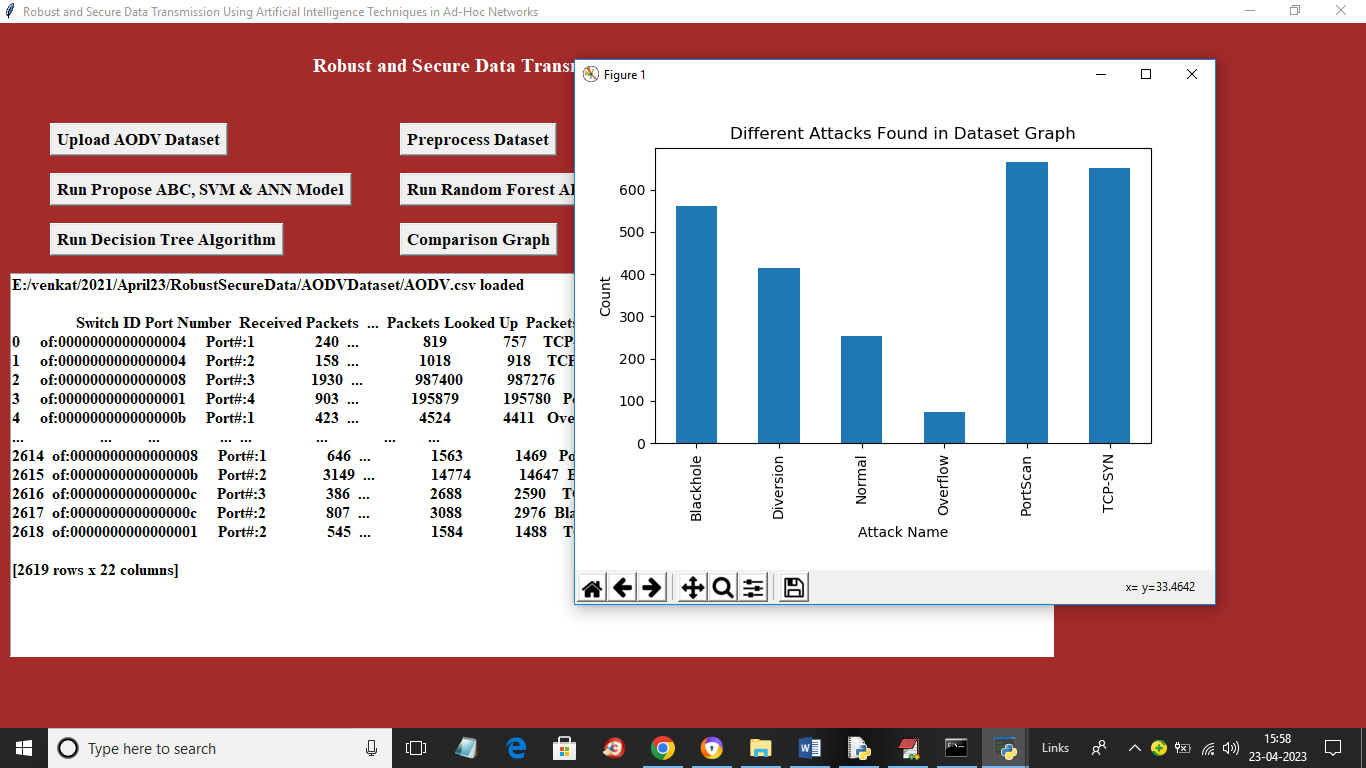
To run project double click on ‘run.bat’ file to get below screen



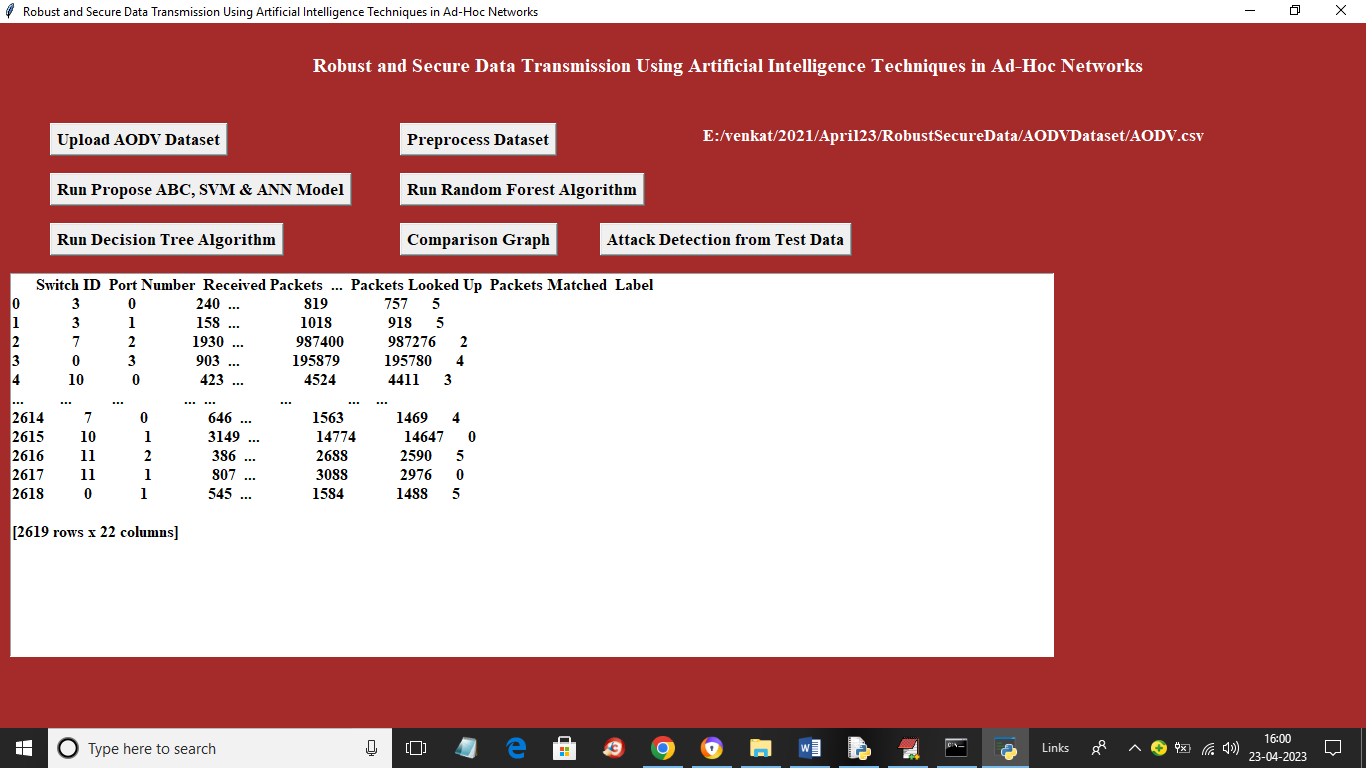
In above screen click on ‘Upload AODV Dataset’ button to upload dataset and get below output



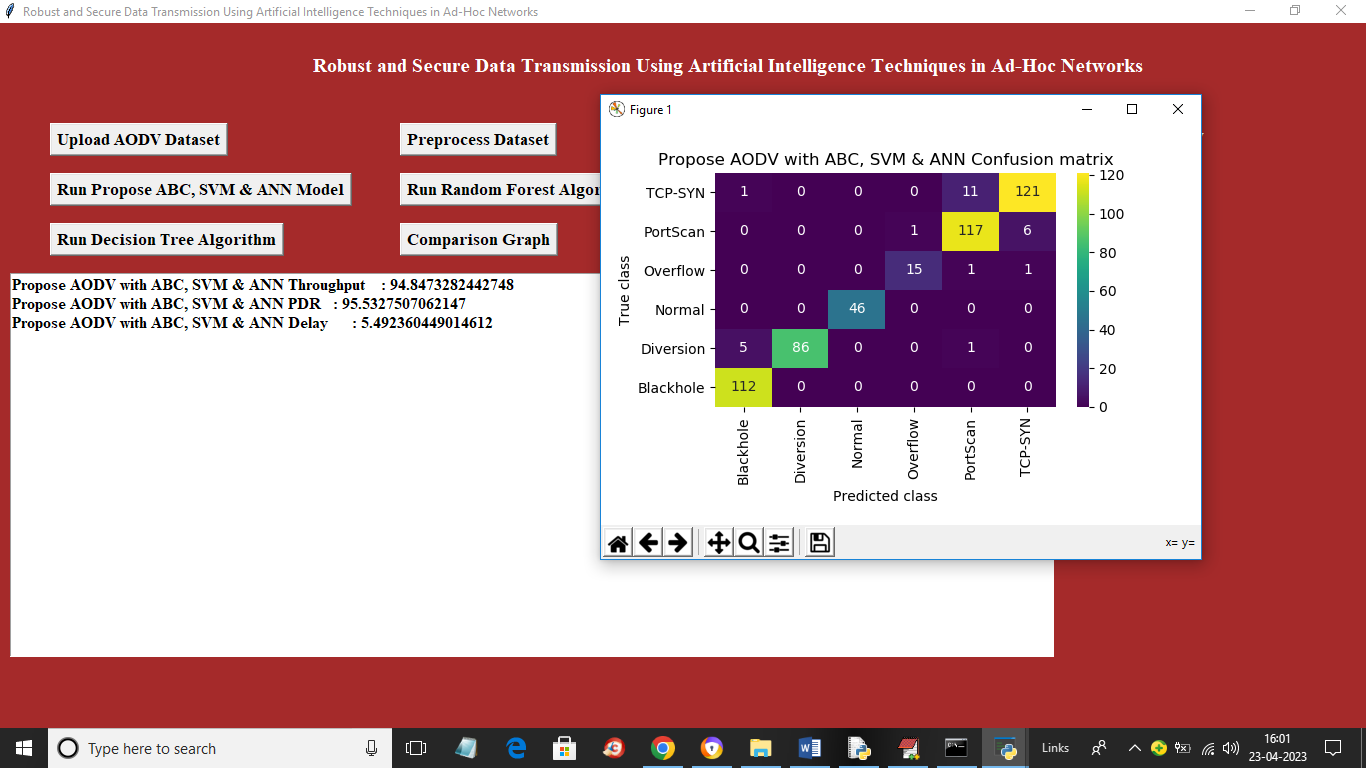
In above screen selecting and uploading entire ‘AODV.csv’ dataset file and then click on ‘Open’ button to load dataset and get below output



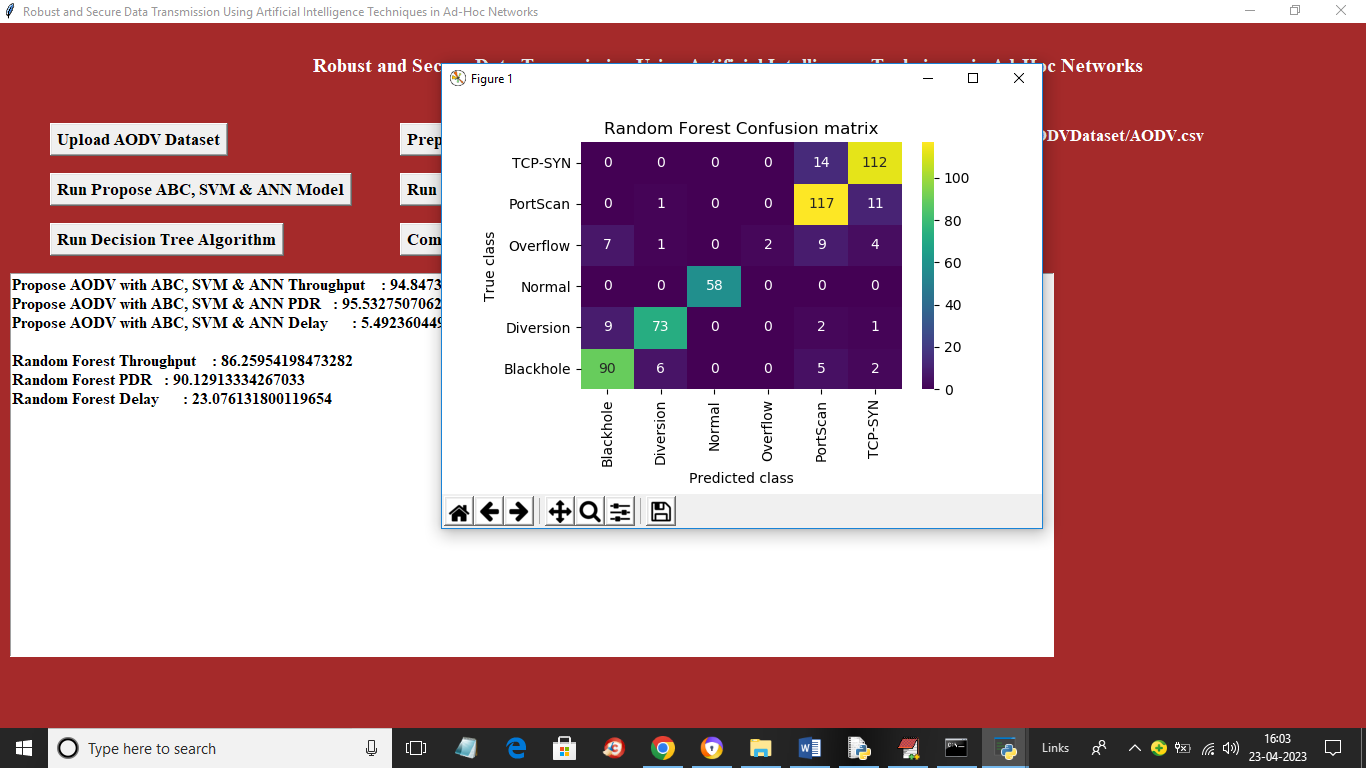
In above screen dataset loaded and we can see dataset contains both numeric and non-numeric data but machine learning accept only numeric values so click on ‘Preprocess Dataset’ button to process dataset and get below output and in above graph x-axis represents ATTACK names and y-axis represents counts and now close above graph and then click on ‘Preprocess Dataset’ button .



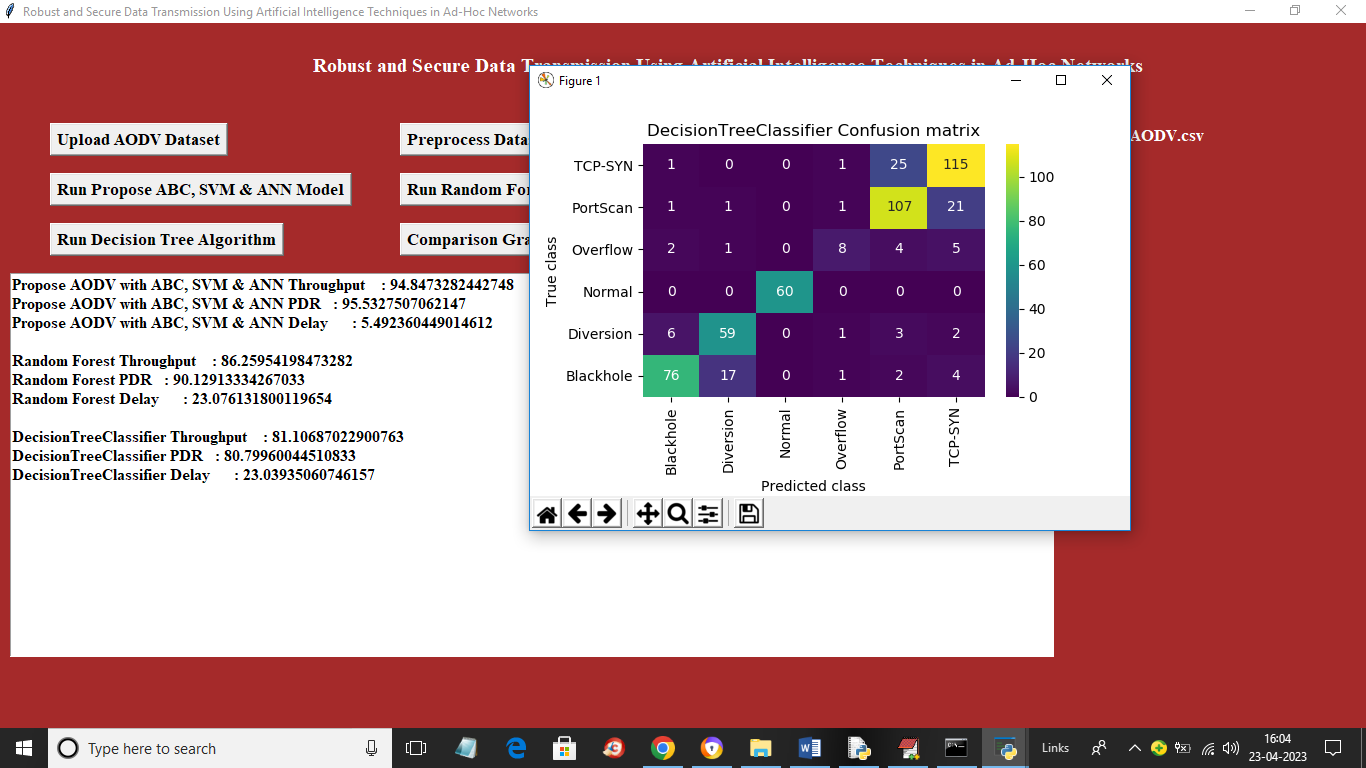
In above screen all non-numeric data converted to numeric data and now click on ‘Run Propose ABC, SVM & ANN Model’ button to train propose algorithm and get below output



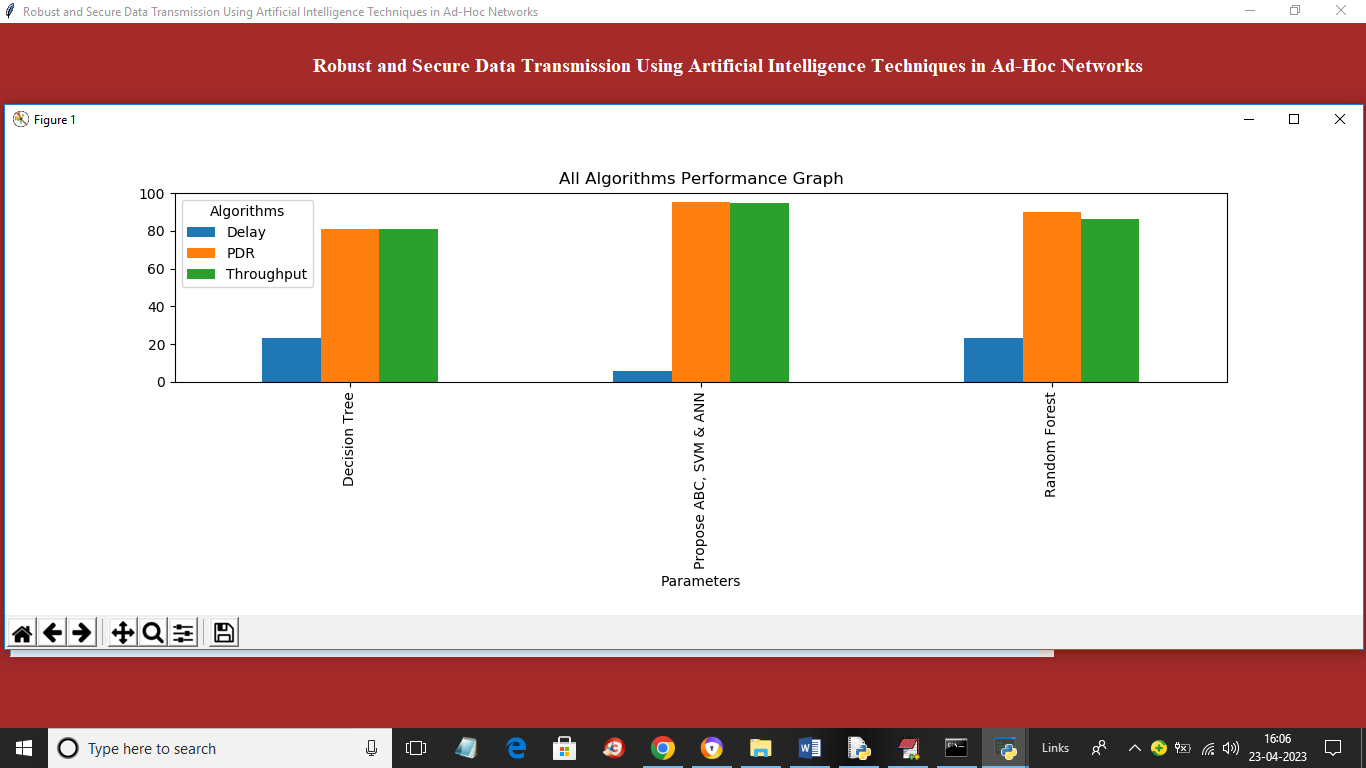
In above screen with propose algorithm we got throughput as 94.84% and we can see other metric also and in confusion matrix graph x-axis represents predicted Attack Names and y-axis represents True Attack Name and all different colour boxes represents correct prediction count and remaining blue colour boxes contains incorrect prediction count which are very few and now click on ‘Run Random Forest Algorithm’ button to train Random Forest and get below output



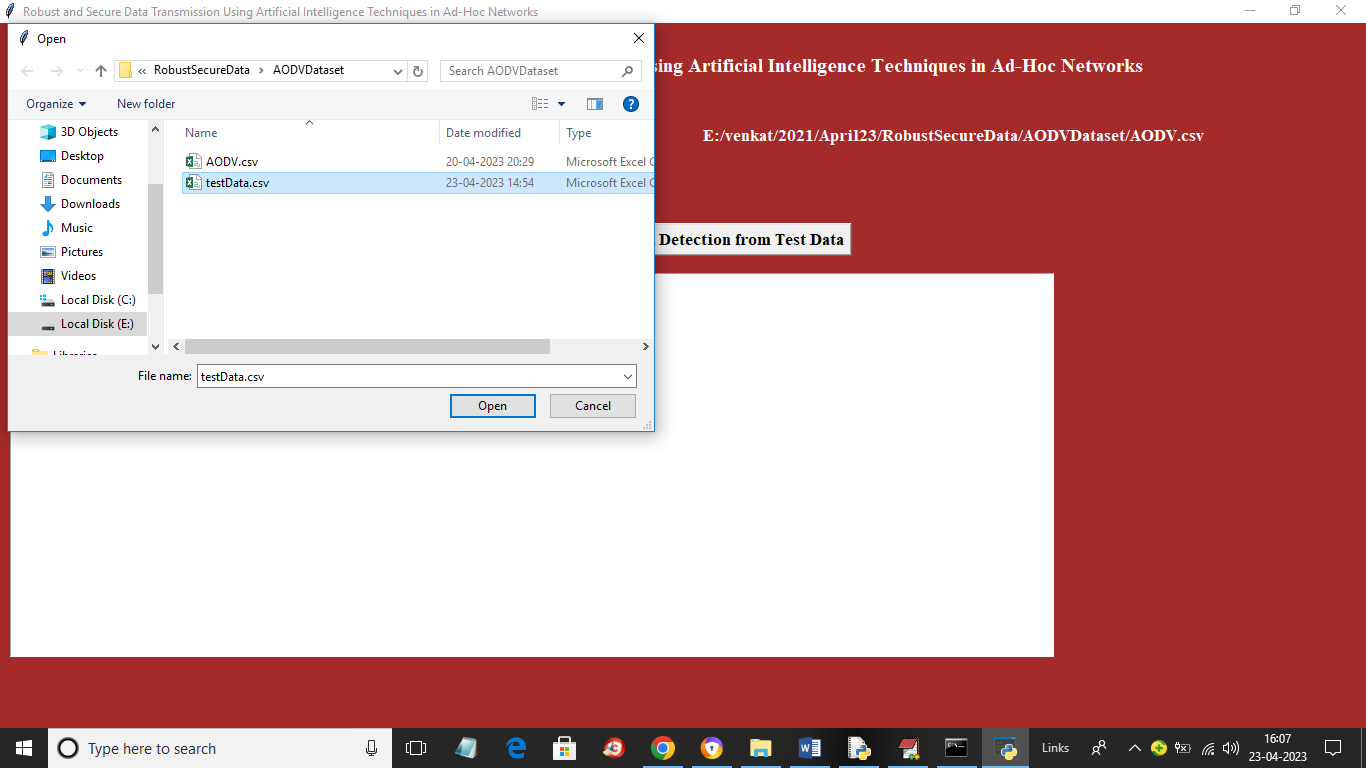
In above screen with Random Forest we got 86% throughput and we can see other metrics also and now click on ‘Run Decision Tree’ button to train decision tree and get below output



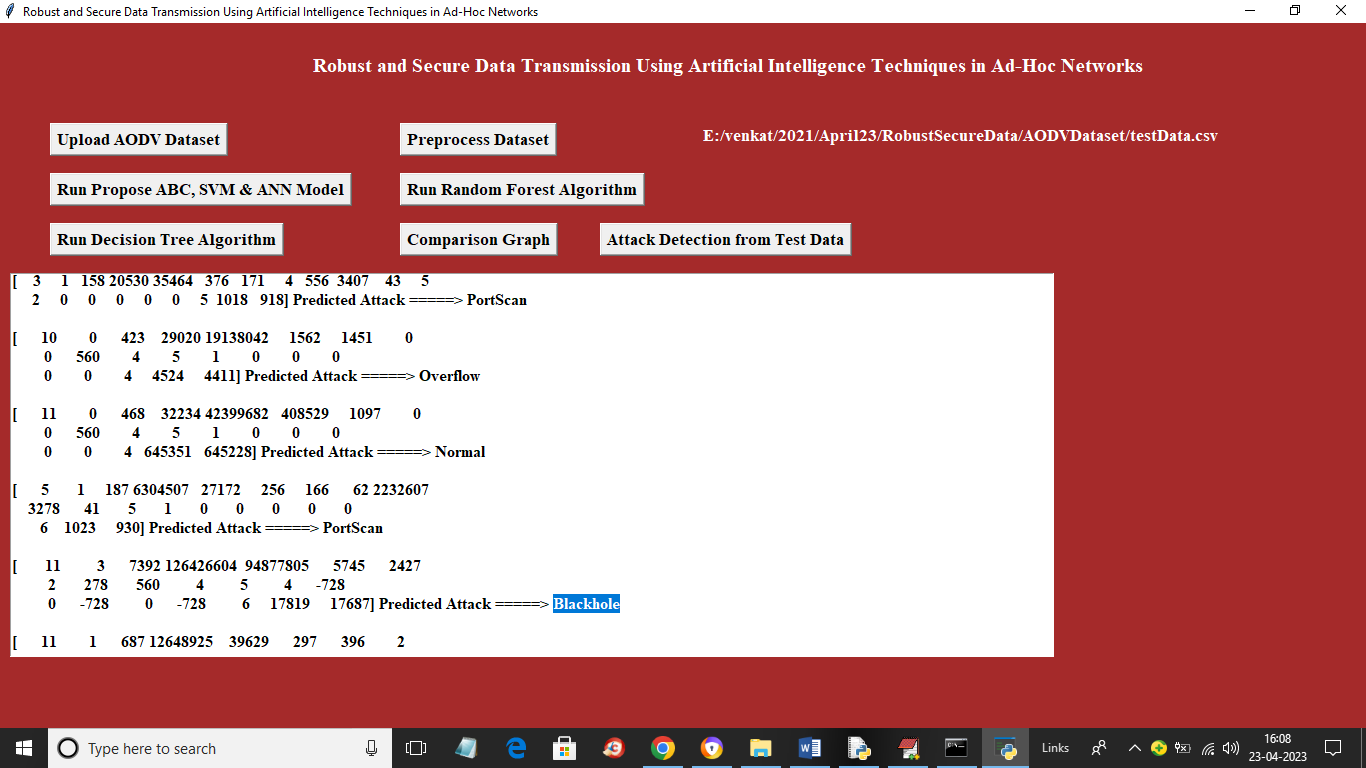
In above screen with Decision Tree we got 81% throughput and now click on ‘Comparison Graph’ button to get below graph



In above graph x-axis represents algorithm names and y-axis represents Throughput, delay and PDR in different colour bars and in above graph Propose ABC + SVM + ANN got high throughput, PDR and less delay. Now click on ‘Attack Detection from Test Data’ button to upload test data and get below output



In above screen selecting and uploading ‘TestData.csv’ file and then click on ‘Open’ button to load dataset and get below output



In above screen in square bracket we can see Test Data and after arrow symbol =🡺 we can see predicted attack names or normal.