Systematic Assessment of Cyber-Physical Security of Energy Management System for Connected and Automated Electric Vehicles

In this paper author is providing security assessment of connected and automatic vehicles (CAEV) under cyber physical attacks. Now-a-days sensors are using everywhere for monitoring and this sensors are using inside various parts of vehicles such as braking system, steering, tyres and other places which will sense data (like slippery tyre or someone comes in front of vehicles) or receive commands from ECU (electronic component units) and perform action based on ECU commands. This devices will work without human monitoring but this advantage raise a security issues where malicious attacker can take control of this sensors and alter their commands. Attacker can issue sudden break apply command or any other abnormal to sensor and execution of such commands by sensors will put person life in risk.

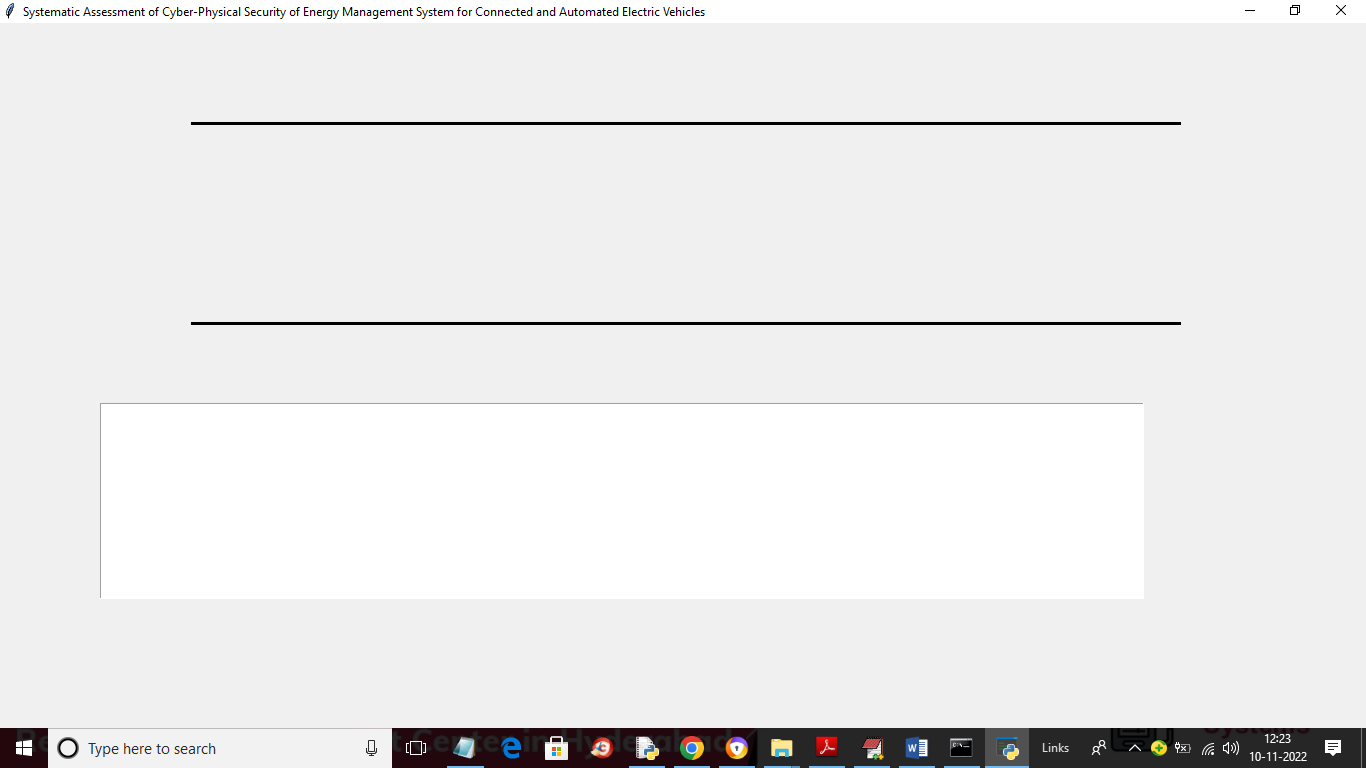
By using malicious commands attacker can raise DOS (by sending enormous request make the resources to be unavailable), replay (send repeated commands again and again). All sensors runs on battery and sending repeated or enormous request continuously may consume more battery. To analyse impact of such attacks and to reduce battery consumption author is assessing energy consumption in various attacks scenarios and then suggesting to avoid such attacks to save energy and this process is called Energy Management System (EMS). EMS can be manage by utilizing technique called Model Prediction Control (MPC).

To predict abnormal or attack condition author is calculating vehicle velocity by subtracting current time vehicle speed with previous time vehicle speed and if there is sudden change in velocity for constant time then the attack will be consider and system will avoid such attacks to save energy and wait till it receive normal commands to get recovered. By avoiding such commands we can save battery consumption and increase vehicle travel time.

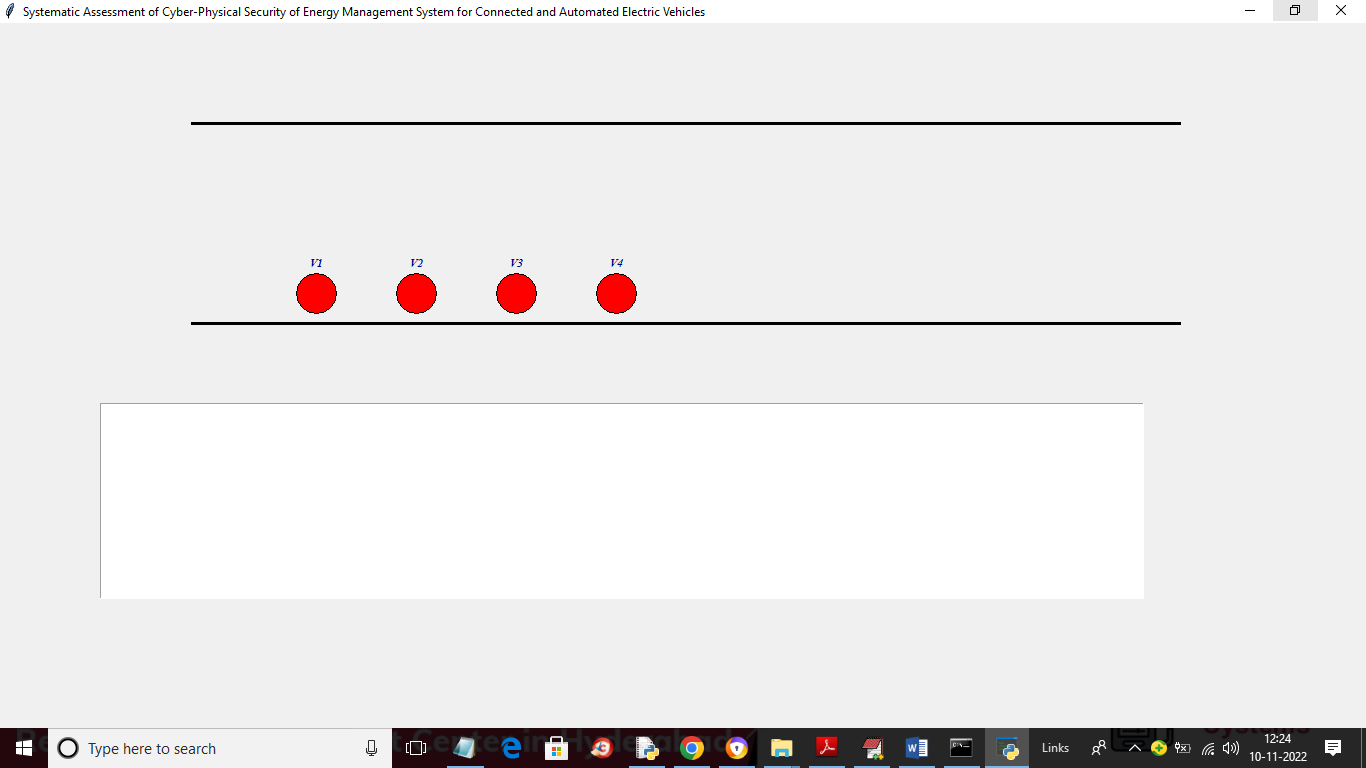
We have designed this application as a simulation where vehicles will move on a road by receiving commands from ECU and then we will monitor vehicle velocity to detect normal and attack scenarios and then record energy consumption in both scenarios.

SCREEN SHOTS

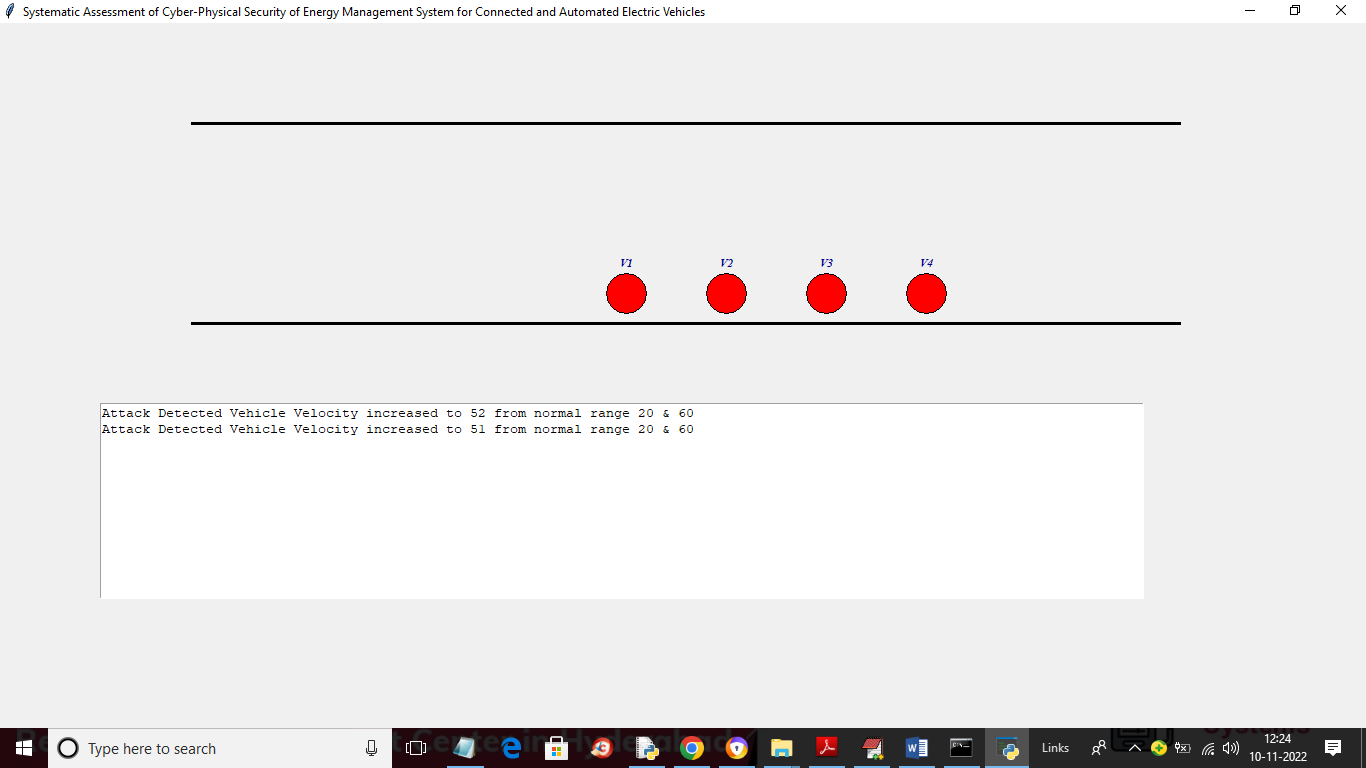
To run project double click on ‘run.bat’ file to get below screen



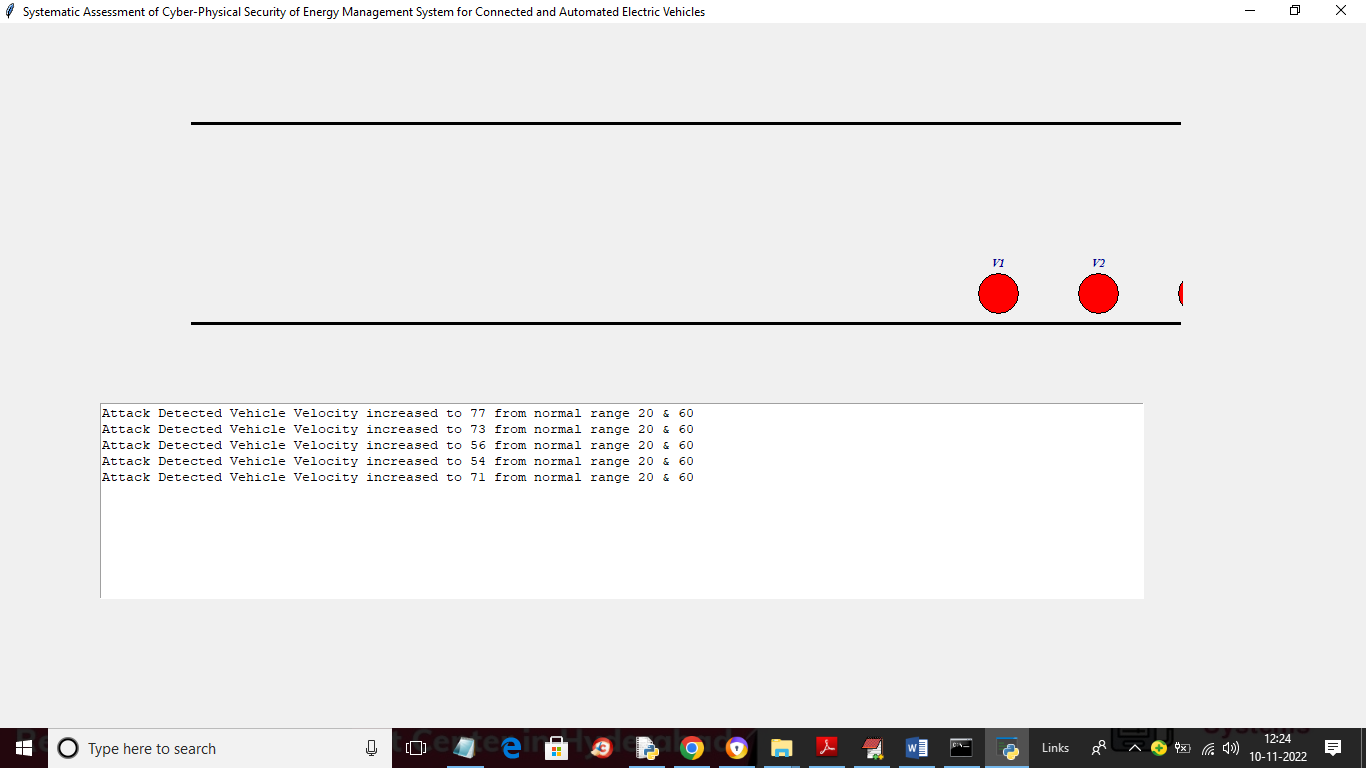
In above screen black lines indicate road and then vehicles will start moving by receiving commands from ECU



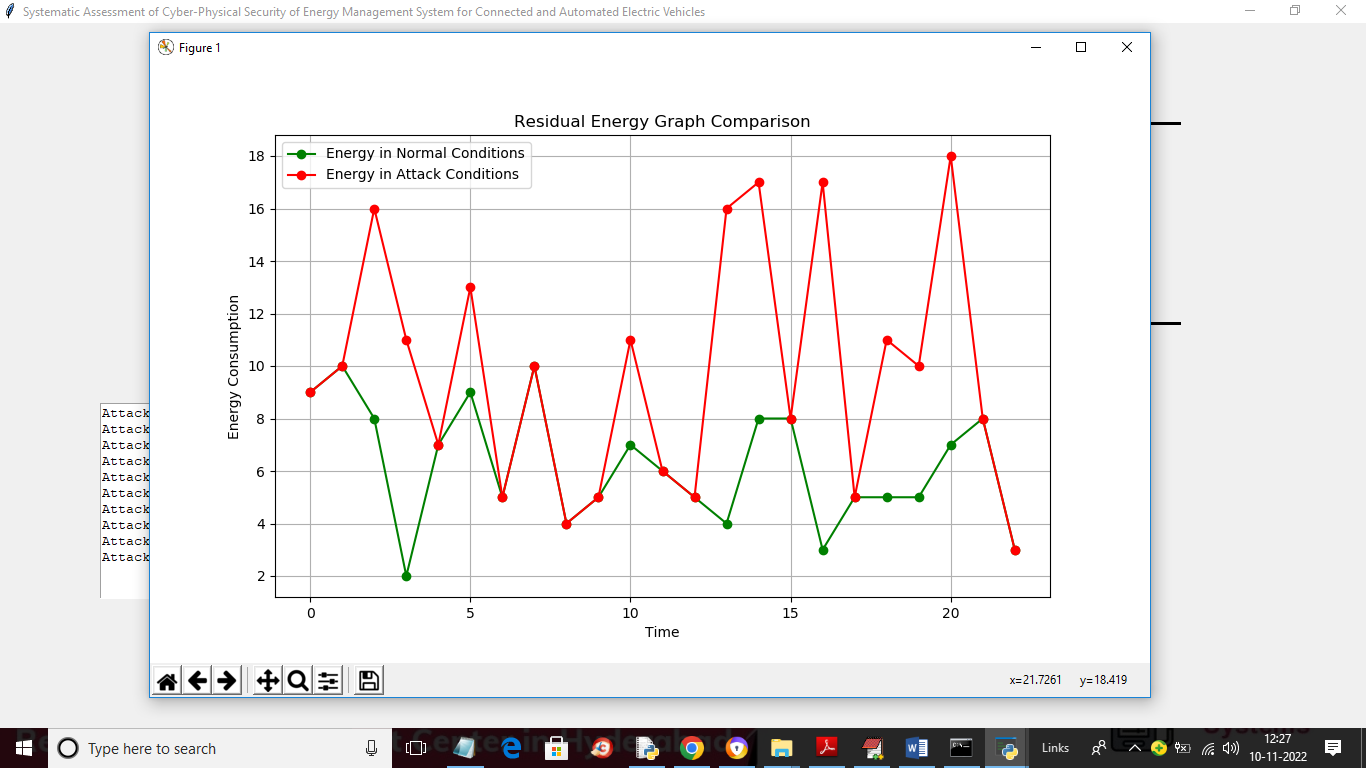
In above screen red colour circles are the vehicles will keep on moving based on commands received from ECU



In above screen in text area we are displaying abnormal command received by vehicles based on velocity. If there is sudden change in velocity from normal range then attack will be detected



In above screen we can see vehicles moving and in text area we can see abnormal commands receive by vehicles. After simulation will get below graph of energy consumption



In above graph x-axis represents TIME and y-axis represents Energy consumption by the vehicles where green line represents energy consumption under normal scenarios and red line represents energy consumption under attack. So by avoiding those DOS and replay attack we can reduced energy consumption up to showing in green line