The Vulnerability of Cyber-Physical System Under Stealthy Attacks

In this paper author is giving mathematical stochastic linear system to detect and classify various attacks such as Strict Stealthy and Stealthy from Cyber Physical System. Strict Stealthy attack is near impossible to detect (this attack can leave some impact to damage or later sensor data even after removal) and Stealthy attack can be detected and leave no impact after detection.

Now-a-days sensors are using everywhere such as Road traffic monitoring, industrial furnace monitoring to control temperature, self-driving vehicle and many more as sensors will sense data from its environment and report to physical server system which analyse this data and then send response back to sensor so sensor will take necessary action. For example in industrial furnace sensor will sense temperature to physical server and server will check if temperature very high then it send command to sensor to cool down furnace. This monitoring will be apply to all types of sensor and due to this sensor monitoring humans are not required to check furnace temperature manually.

This advantages lead to another problem where malicious attacker may inject false reading to sensor and then sensor will send false data to physical server and physical server may take wrong decision and may leads to losses.

To overcome from above attacks author of this paper using stochastic system which monitor state (EIGEN values)of each sensor data and if this data is in normal range including NOISES then no attack will be detected. If attacker inject closed data to normal range then it’s difficult to identify it as Noise data or STRICT STEALTHY attack. So this strict stealthy attack is near impossible to detect so if we remove such attack then it may be noise or attack data and if we don’t remove then it will still impact the system.

Eigen state values which are not too closes to normal range will be consider as STEALTHY attack and this attack can be removed and will not leave any impact on the system after removing.

This normal sensor state range values can be given default as threshold for example for temperature we can put normal range values between 15 to 45 and for different sensor different normal range values can be set. Based on this normal range values attacks can be classified

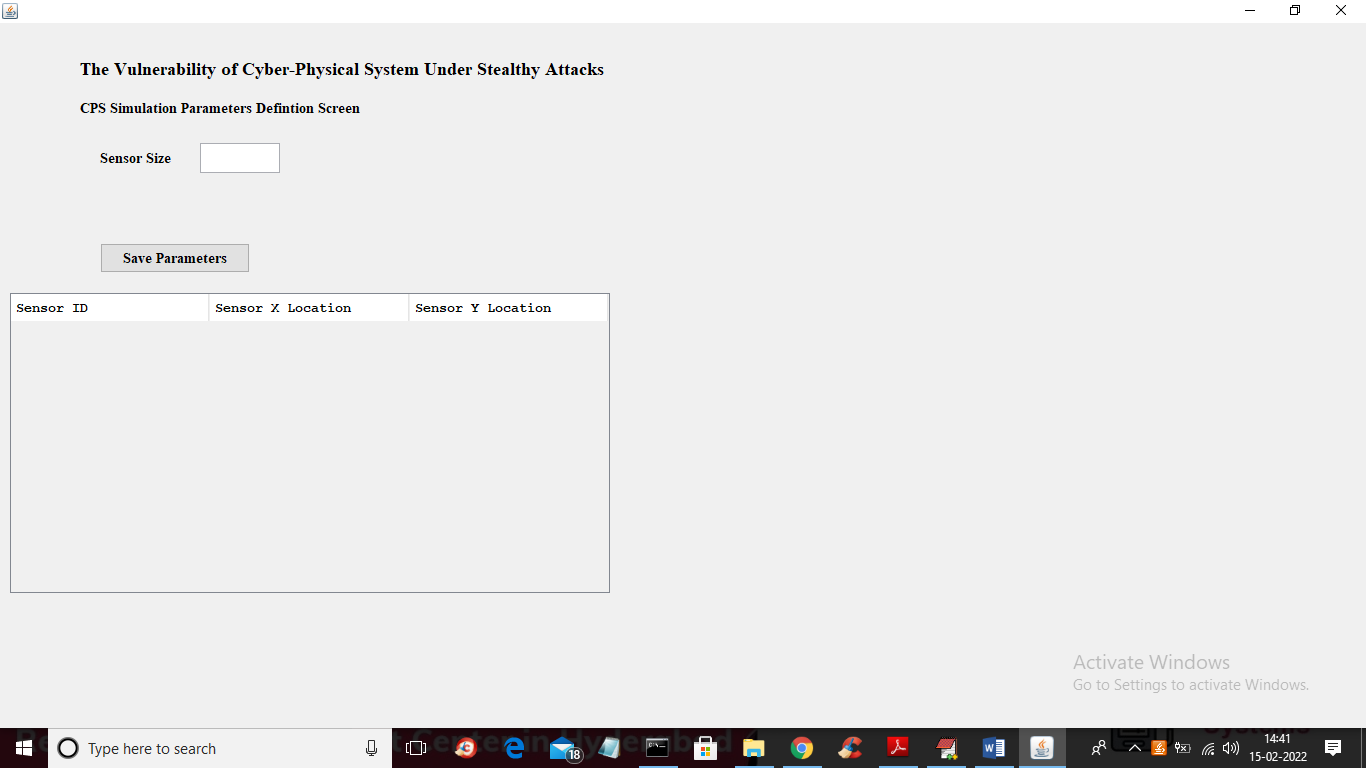
To implement this project author has done simulation so we are also implementing this project as JAVA sensor simulation

To implement this project we have designed following modules

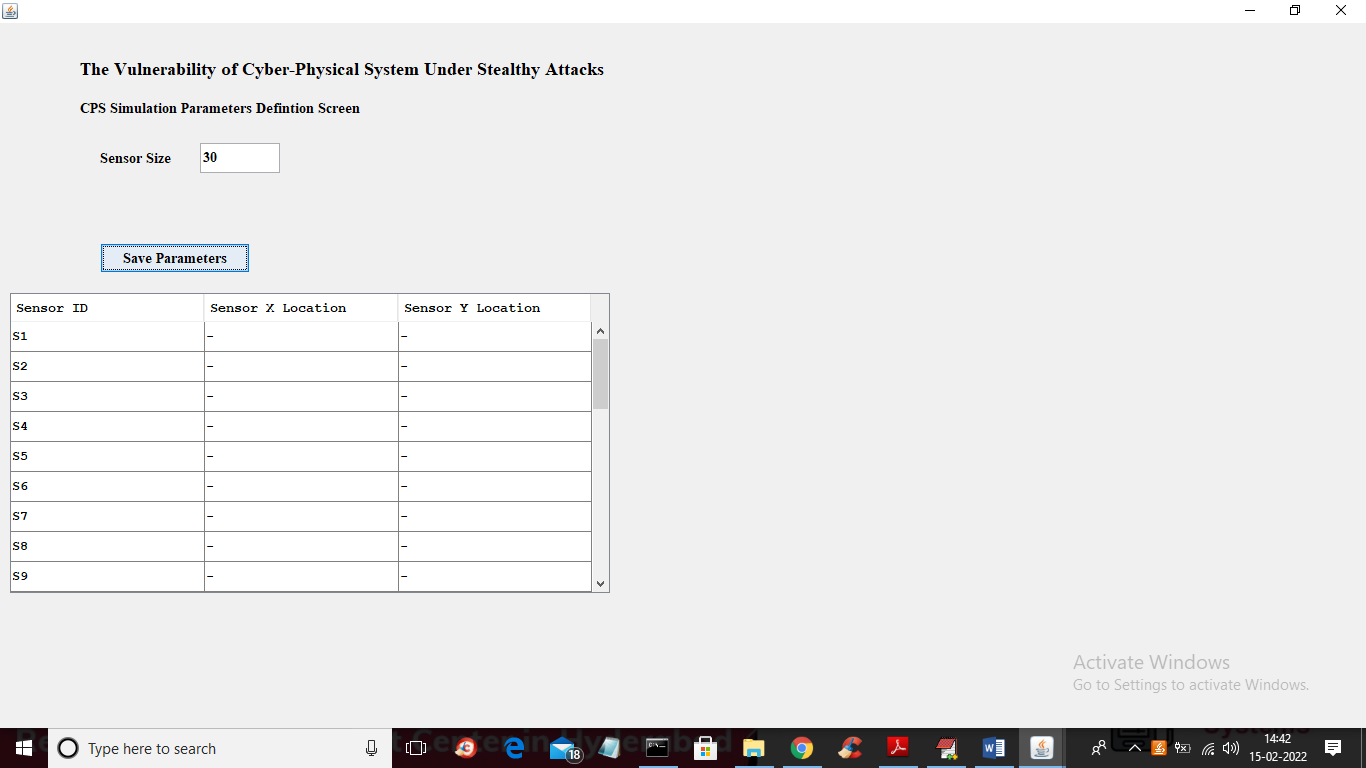
1. Sensors Placements: using this module we will plot sensor on different areas of the screen
2. Start Simulation: using this module we will start simulation where each sensor will sense data and then report to CPS (cyber physical system) and while running we are injecting false or attack data and then system will classify such attack data as normal, STRICT STEALTHY or STEALTHY
3. Stop Simulation: using this module we will stop the simulation
4. Strictly & Stealthy Attack Detections: using this module we will plot different sense packets received graph such as normal packets, total packets and attack packets.

SCREEN SHOTS

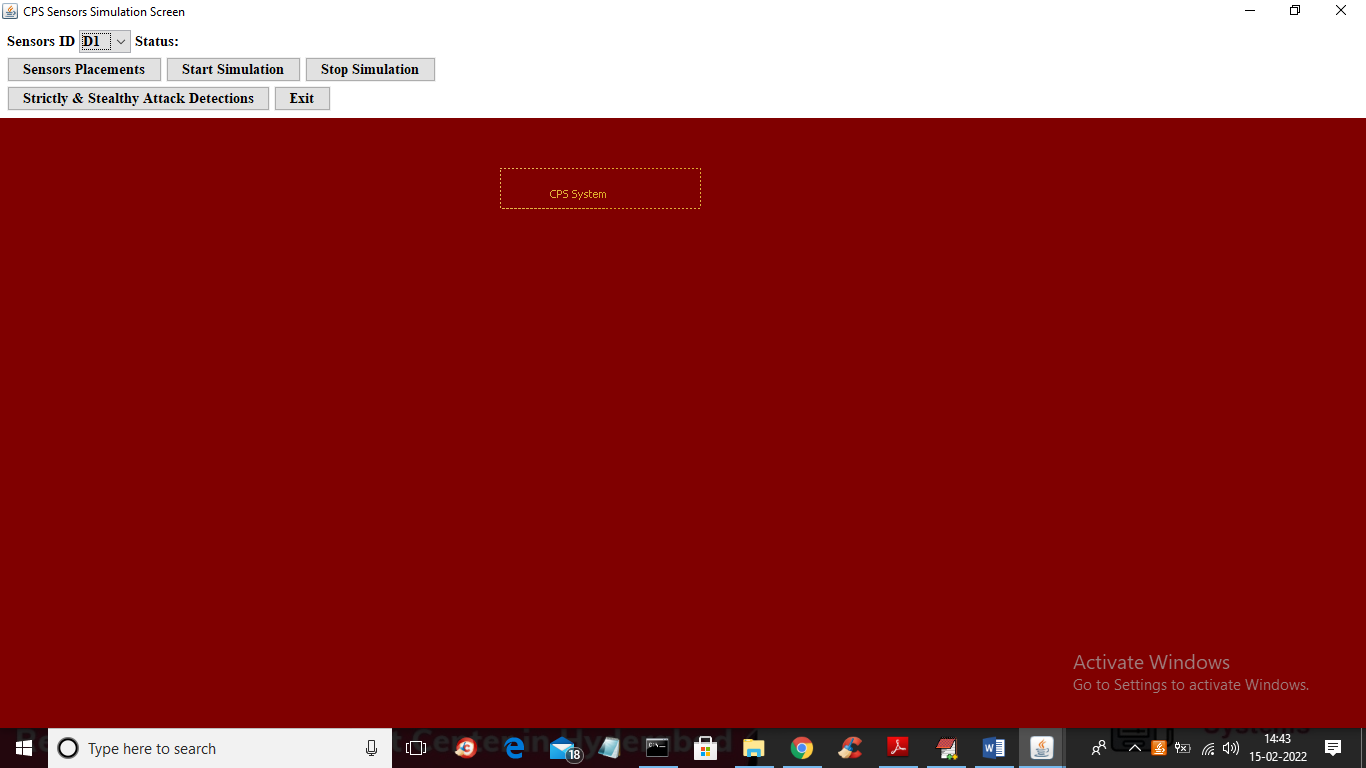
To run project double click on ‘run.bat’ file to get below screen



In above screen enter number of sensors in first text field and then press “Save Parameters” button to get below screen



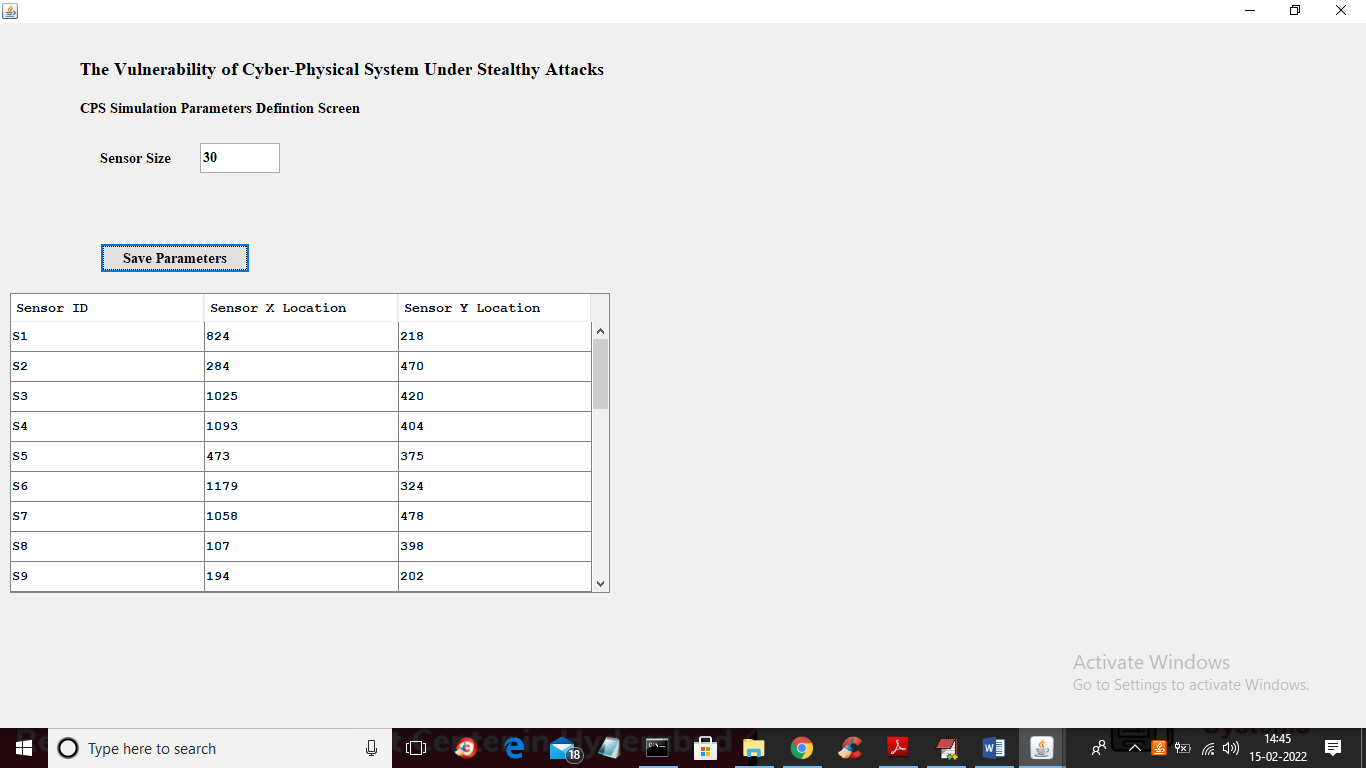
In above screen I entered number of sensor as 30 and then click on button to generate that many sensors to get below screen



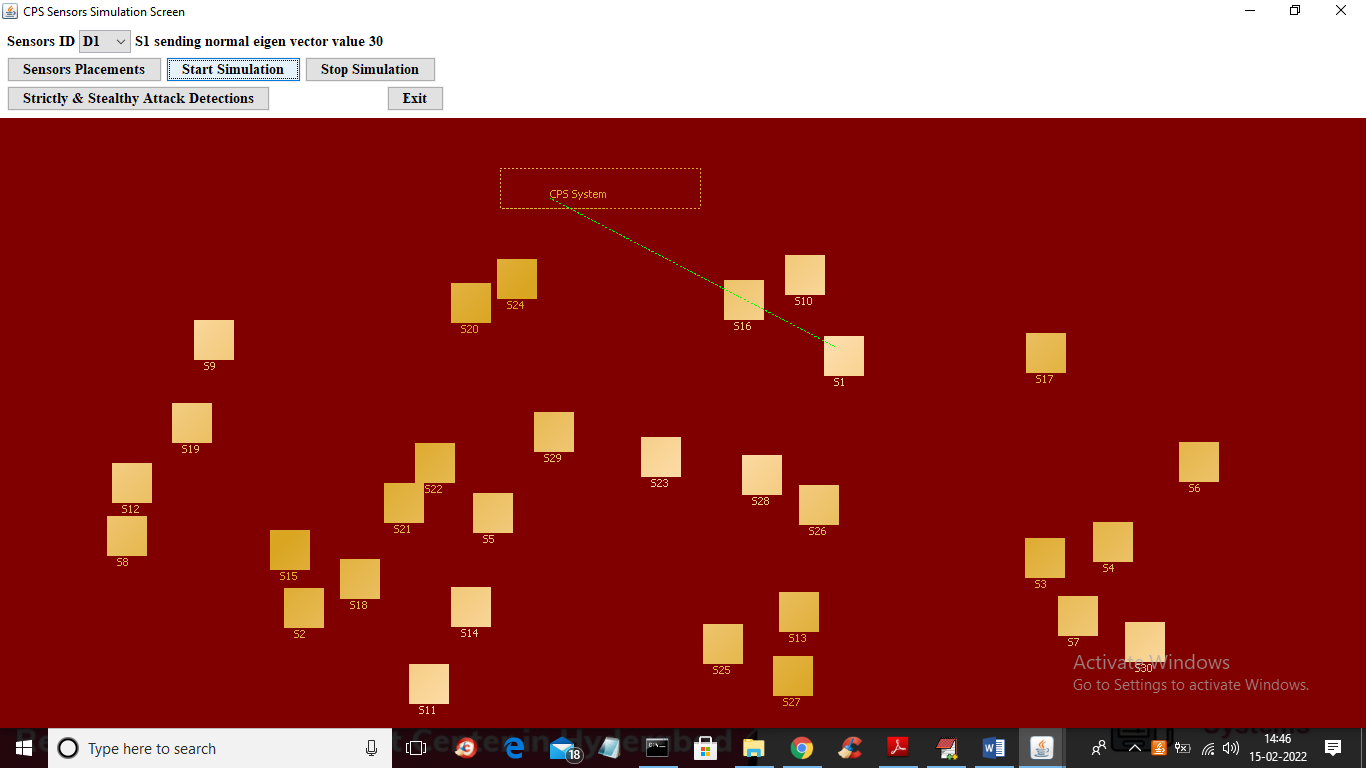
In above screen click on ‘Sensors Placements’ button o place 30 sensors in different region of the screen and will get below screen



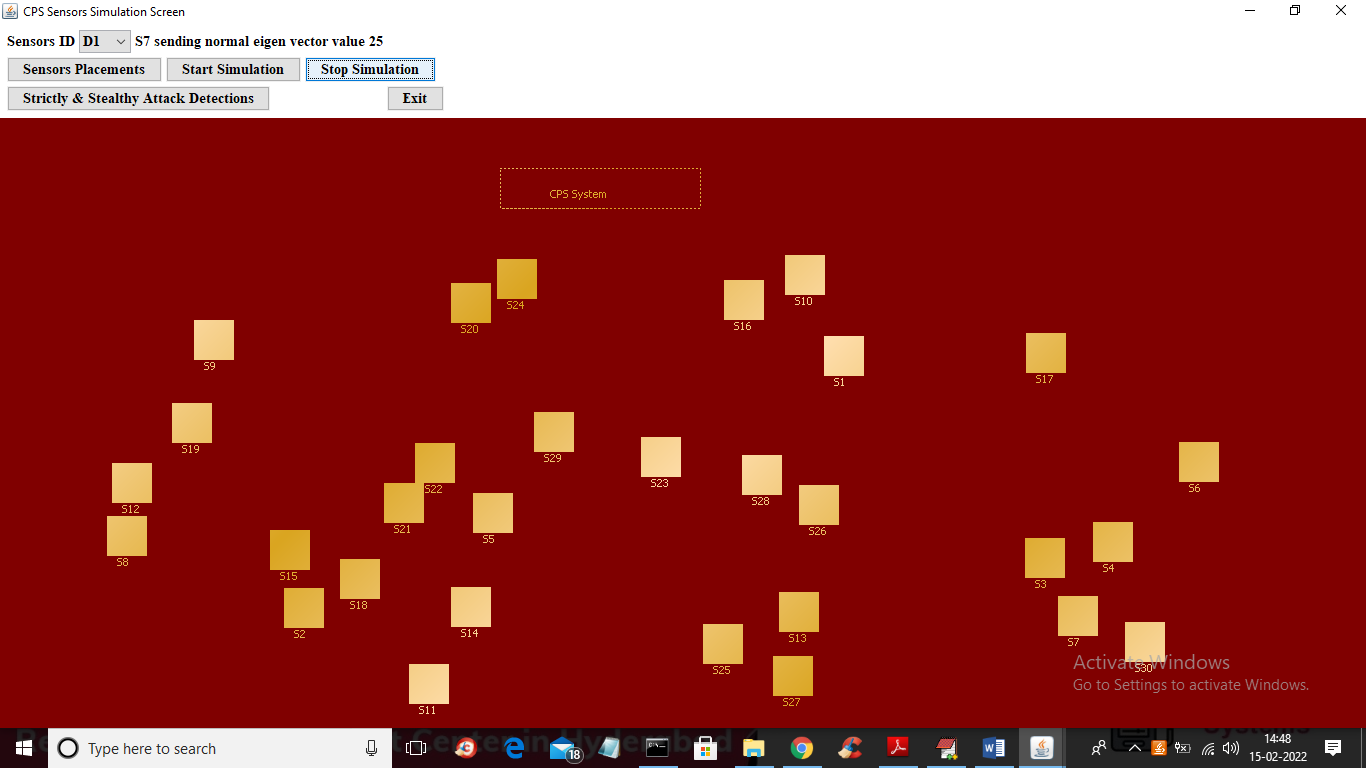
In above screen each small rectangle will be consider as one sensor and big dotted rectangle will be consider as CPS system which will received data from sensors and process and then detect it as normal or attack data. IN below screen we can see X and Y location of each sensor



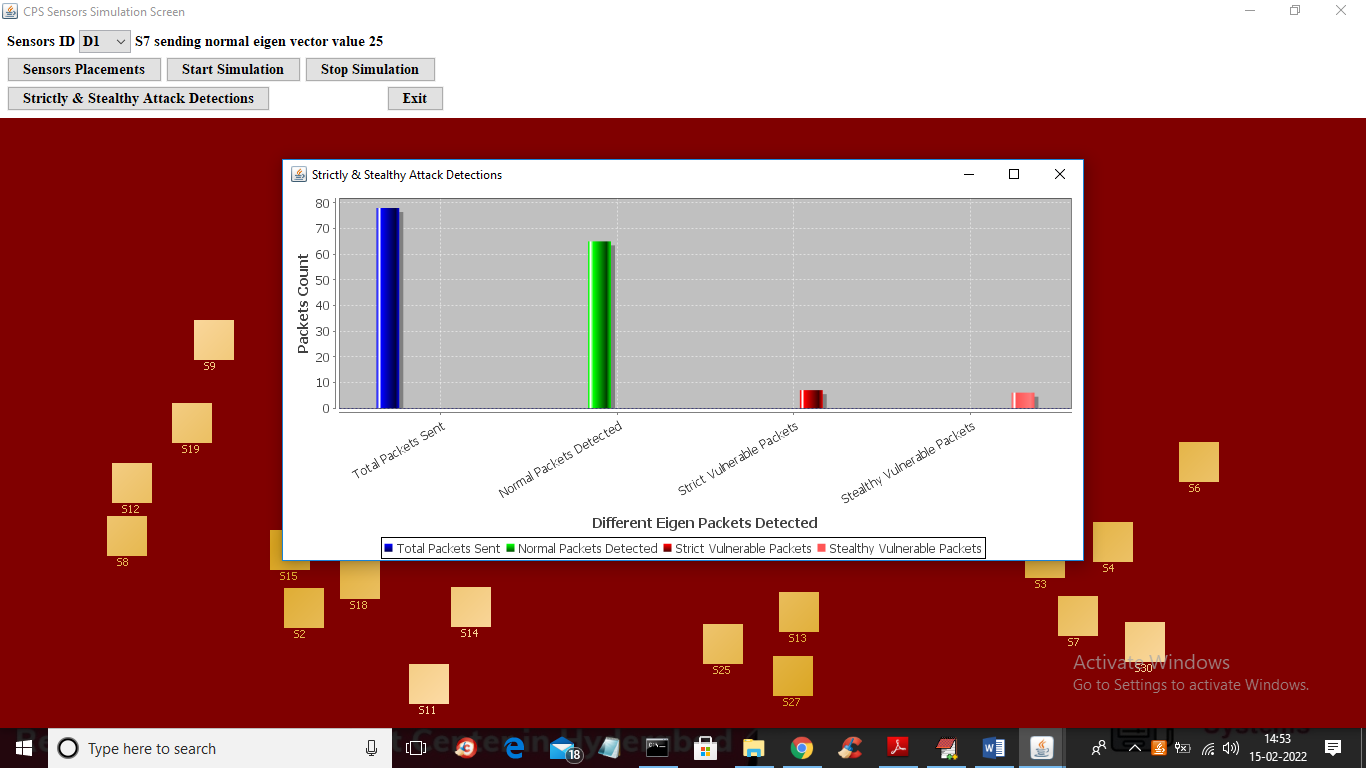
In above screen we can see X and Y locations for each sensors and now in previous screen click on ‘Start Simulation’ button to start sending data to CPS system



In above screen each sensor will sense data and then send to CPS system and it will send data by using line connecting between CPS and sensor. If sensor data is normal then GREEN LINE will come and if sensor data detected as STEALTHY attack the BLUE line will come and if data is detected as STRICT STEALTHY attack then RED line will come. Now you can click on ‘Stop Simulation’ button to stop the simulation



In above screen we can see simulation is STOPPED and now click on ‘Strictly & Stealthy Attack Detections’ to get below graph



In above graph x-axis represents types of packets sent by sensors and then those packets will be classified as NORMAL, STEALTHY or STRICT STEALTHY attack.

Here injecting false data to sensor packets will be consider as stealthy