* Extended Kalman filter (EKF) based mechanism to detect false injected data
  + Each node aims to set up a normal range of neighbor’s future transmitted aggregated values
* Cumulative summation (CUSUM) and generalized likelihood ratio (GLR) is used to increase detection sensitivity when malicious values have small deviations
  + Because deviations from predictions are summed up
  + Weakness of CUSUM is that it incurs computation overhead to resource-constrained nodes
* GOAL: Break CUSUM
* Attack Scenario:
  + Many examples online talk about DOS
  + Traffic Monitoring
  + Military applications i.e. measuring levels of gas concentrations in battle fields
  + Aimed to disrupt the functioning of system by compromising sensor nodes
  + Increase the temperature of the room to cause damage
* **How to figure out how the measurements would look like in the attack. High temperatures.**
* **If trying to depict something which is a rising phenomenon, should look for measurements that are… Make sure some of these datasets are normal… Think of a scenario where in a particular state, this can be normal, or abnormal. Make a list of possible situation which could happen.**
* **A possibility where an attacker wants to create a false alarm. Plot the dataset to see if it looks like a fire. But unlikely because it’s a lab dataset. Look at other dataset. Vittorio has dataset for fire alarm. Attack tries to mimic or replicate. Think about other kinds of scenario i.e. attacker can do that or this. Ie. Fire.**

**Questions**

* Which dataset should I use?