Machine Learning Techniques to Detect GPS Spoofing Attacks in the Wide-Area Monitoring System (WAMS) for Power Systems

The increasingly pervasive installation of Phasor Measurement Units (PMUs) in recent years has dramatically changed the landscape of power grid monitoring and control. To date, there are 2,500 PMUs at key locations of North American power grid, such as major transmission inter-connections, key generation plants, substations, and major load centers to form a wide-area monitoring system (WAMS) for our power grid. More and more control room applications are starting to integrate these high-resolution synchronized measurements to improve the grid reliability and efficiency. However, this also introduces great concerns about the cyber security of the synchrophasor measurements generated by PMUs. The civilian GPS signal utilized in PMU is publicly known and readily predictable, and this makes GPS-based timestamp synchronization vulnerable to GPS spoofing attack (GSA), which hijacks the PMU by faking the GPS signal and compromises the reliability of all the synchrophasor data provided by this PMU.

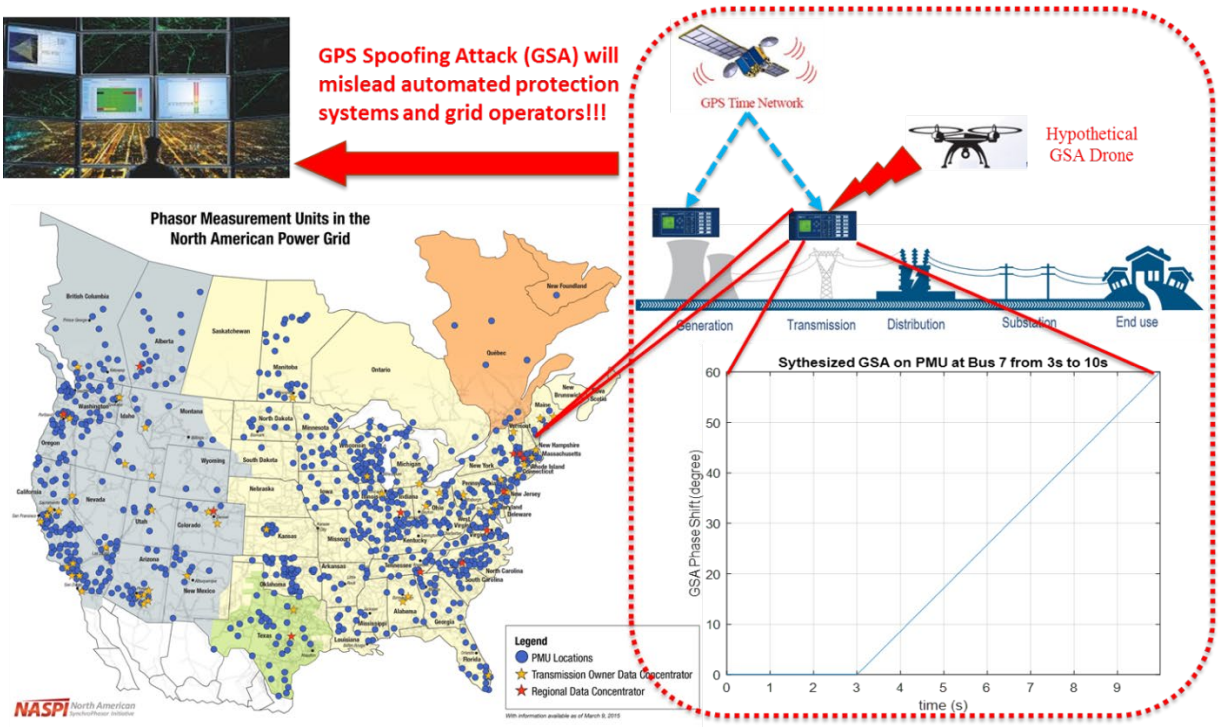

Figure 1: A hypothetical GPS spoofing attack scenario.

This mini project aims at improving the cyber-resilience of power grid operations and applications that rely on GPS-based timing. This is achieved by online detection of GPS spoofing attacks (GSA) and incorporation of adaptive remedial actions for this kind of cyber-attack. The main idea is to apply machine learning techniques on the historical data to build a general model for the normal operations of the WAMS and then conduct online detection of GPS spoofing attacks by checking the discrepancy between the online measurement data reported by the PMUs and the trained model.