Securing Smart Grids and Buildings Infrastructures and Services

Jesus Horacio Pacheco Ramirez, Bilal Al Baalbaki, Jin Bai, Zhiwen Pan, Youssif Al Nashif and Salim Hariri

http://acl.ece.arizona.edu/projects/current/aimsg/index.html

Problem

- The development of Smart Grids is strongly linked to the utilization of technology that has the capability of enhancing system performance, reduce costs, and introduce new services by interconnecting (e.g. ZigBee, Wi-Fi, DNP3, BACNET) with internet (IoT). The problem arises when the system is directly exposed to attacks. Our goal is to build an effective intrusion detection system that can proactively detect anomalous actions generated by malicious devices from inside or outside networks.

Solution

- To automate any software module or resource, we add two software modules: **Observer and Controller**
  - The Observer is used for sensing and analyzing the current state of managed system and predict its behavior.
  - The controller executes recommended actions to keep the managed system operating normally (self-manage).