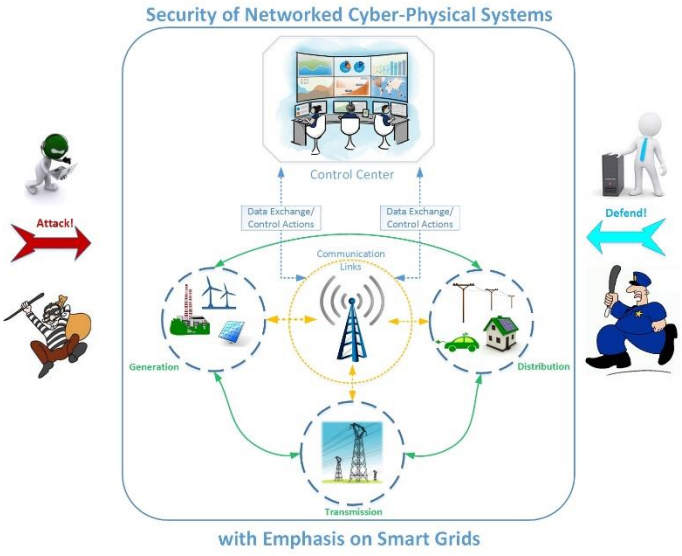
Security of Cyber Physical Systems

Security of Networked Cyber-Physical Systems with Human Decision Makers:

Student: Anibal Sanjab (PhD Student)

Our research work in this area focuses on developing novel mathematical principles to design secure and robust networked cyber-physical systems (NCPS) with applications to multiple CPS domains such as power systems, transportation systems, and the Internet of things.

Our goal is to better understand the security of networked cyber-physical systems and more importantly recognize the role of humans, their behavior, partial rationality, interaction and decisions, on the security of NCPS. In this regard, a key component of our work is to apply novel game theoretic models and control systems theory to better integrate the cyber and physical layers of networked systems while focusing on the role of humans and the effect of their behavior and interaction on the security of the joint CPS.



One of the first topics we considered, focused on the problem of stealthy data injection attacks on smart electric grids with multiple potential attackers. We analyzed the strategic interaction between those various attackers and the system defender through a game-theoretic model. The problem was formulated using a Stackelberg game in which the defender acts as a leader that can anticipate the actions of the adversaries that act as followers, before deciding on a subset of communication links to protect against data attacks. Our work has provided valuable insights on how data injection attacks with multiple adversaries can impact a smart grid. In fact, we have proven that the adversarial nature of the attackers can impact the effectiveness of each other's attack strategies reducing the aggregate effect of the attacks on the smart grid. This work appeared in the IEEE Smartgridcomm 2015 conference. Currently, we are looking at various avenues that extend this and other work, in an effort to develop fundamentally new frameworks for understanding the security of complex and large-scale cyber-physical systems.