Title of Thesis: “**Moving Target Defence for Securing Smart Grid Communications**”

*Abstract:*

 Supervisory Control And Data Acquisition (SCADA) communications are often subjected to various kinds of sophisticated cyber-attacks which can have a serious impact on the Critical Infrastructure such as the power grid. Most of the time, the success of the attack is based on the static characteristics of the system, thereby enabling an easier profiling of the target system(s) by the adversary and consequently exploiting their limited resources. In this thesis, a novel approach to mitigate such static vulnerabilities is proposed by implementing a Moving Target Defence (MTD) strategy in a power grid SCADA environment, which leverages the existing communication network with an end-to-end IP Hopping technique among the trusted peer devices. This offers a proactive L3 layer network defence, minimizing IP-specific threats and thwarting worm propagation, APTs, etc., which utilize the cyber kill chain for attacking the system through the SCADA network. The main contribution of this thesis is to show how MTD concepts provide increased attack resiliency, proactive defence, and a dynamic attack surface to adversaries without compromising the availability and reliability of a SCADA system.

Specifically, the thesis presents a brief overview of the architecture and implementation of the MTD using IP hopping technique over a Control Centre–Substation network link along with a 3-way handshake protocol for synchronization on the Iowa State’s Power Cyber testbed. The thesis further investigates the delay and throughput characteristics of the entire system with and without the MTD to choose the best hopping rate for the given link. Finally, the thesis describes different case studies to explore and identify potential weaknesses of the proposed mechanism, and also experimentally validate the proposed mitigation alterations to resolve the discovered vulnerabilities. As part of future work, we plan to extend this work by optimizing the MTD algorithm to be more resilient by incorporating other techniques like network port mutation to further increase the attack complexity and cost.