

Protecting the Future of our Critical Infrastructure: Novel Approach Towards Understating Disruptive Network, Communication, and System Technologies

Developing a skilled diverse workforce with the knowledge to protect our future critical infrastructure (i.e., power grids, transportation, water, gas and oil, and other systems) is a serious challenge because of its complexity and high demand for specialized workforce skill set normally taught at a few academic institutions. Thus, there is gap between disruptive and innovative technologies that can to solve the problems and the demand for a qualified workforce in cybersecurity that will provide safety for our future critical infrastructure. Workforce development and readiness at diverse academic institutions like our current institution is usually developed via internship/co-ops, which not all students have access or even know how to obtain and be prepared for. Also, students need to develop research, communication, problem solving, and critical thinking skills under a real-world perspective.

We have explored this challenge during our previous research by providing opportunities inside and outside of the classroom for students to be actively engaged in their learning process using the Affinity Research Group (ARG). ARG is used to teach research skills, create a safe environment for students and collaborators to become lifelong learners, leaders, and create community. Additionally, ARG involves and engages students in research

projects that range from how to use testbeds/equipment for network experimentation as well as using wireless networks to monitor critical transportation infrastructure such as bridges. Thus, building on the success of our previous research, our current research seeks to understand how to better prepare students to have research skills and be workforce ready to protect our critical infrastructure. Particularly, we would like to explore and understand/experiment disruptive network and systems technologies using testbeds. For example, we are very interested in learning how disruptive communication infrastructure technologies such as Software Defined Networks (SDN) and P4 programming language can be used to automat the protection, measurement, and

monitor network infrastructure safety. Current network infrastructure is the basic communication mechanism that supports our future critical infrastructure. Innovations in SDN, P4, and other technologies may solve many

of the existing problems but they may also bring new vulnerabilities not considered before. T. Dargahi and et at.

study the security implications and vulnerabilities of these technologies when used to communicate user data across the networks (T. Dargahi, A. Caponi, M. Ambrosin, G. Bianchi, and M. Conti. IEEE Communications Surveys & Tutorials 19 (3), 1701-1725, 2017). We will like to expand on their work and understand better these technologies.

(download PDF for full text)

Primary author: PERERA, Graciela (NIU)

Presenter: PERERA, Graciela (NIU)