Un-hackable Communications with Quantum Key Distribution for Secure Remote Operations

PI: Dr. Stylianos Chatzidakis – Purdue University

Program: Crosscutting Research – Cyber Security Research, CT-1

Collaborators: Dr. Lefteri Tsoukalas – Purdue University
Mr. Clive Townsend, Purdue University Reactor (PUR-1)
Dr. Joseph Lukens – Oak Ridge National Lab
Dr. Sacit Cetiner – Oak Ridge National Lab
Dr. Phil Evans – Oak Ridge National Lab

ABSTRACT:

The first new passive advanced nuclear systems are designed to be smaller—both in size and power output—than the commercial nuclear plants in operation today, and will enable unattended and autonomous operation in remote areas, e.g., microreactors and fission batteries. These characteristics require more universal data collection and sharing as well as cutting-edge instrumentation and increased dependency on digital technologies. While this architecture offers numerous advantages, it is nevertheless vulnerable to cyber attacks. Independent of the objectives or aims of an attack, attackers almost always first gather information about the target system to identify network topology, software versions, and critical targets. This highlights that the first critical layer of defense against attacks would be to guarantee the confidentiality and authentication of any communication.

To address this, current efforts rely on traditional Information Technology (IT) measures such as isolating or minimizing intrusions (e.g., firewalls and data diodes) or intrusion detection measures (e.g., network traffic monitoring). While these efforts have the potential to improve the security of future nuclear communications, significant vulnerabilities remain. Not all cyber attacks are detectable by current intrusion prevention or detection systems that monitor network and host system data. For example, attacks aiming to gather sensitive information about the target system to identify network topology, secret keys, software vulnerabilities, and critical targets often do not leave a trace. We currently lack the technologies needed to detect and defend against these untraceable intrusions into nuclear systems to enable secure communication solutions for future reactor technologies.

To fill this critical gap, we will leverage and demonstrate a new revolutionary quantum-based cyber security technology, Quantum Key Distribution (QKD). QKD secured communication can ensure protection against traditionally untraceable external attempts to expose critical information. Classical encryption systems depend on the computational difficulty of mathematical functions and have been shown to be vulnerable to attacks—especially with the advent of quantum computing. In response, QKD exploits the fact that a measurement disturbs the state of a quantum mechanical system and that a random unknown quantum state cannot be cloned. This is unique to quantum mechanics and can be used to detect if someone "eavesdropped" during the encryption process and if so, how much information was gained by the eavesdropper.

In this project, we will develop quantum-based secure communication architectures optimized for QKD protocols in advanced nuclear systems and demonstrate their use on Purdue's all digital University Reactor, PUR-1, the first reactor in the U.S. with fully digital instrumentation and control. Access to, and deep knowledge of, this facility coupled with QKD equipment will provide a unique opportunity to implement and study a secure communications network under prototypic conditions.