ASSURING RESILIENCE OF GRID TIMING UNDER CYBER STRESS

FOR THE NATION'S ENERGY SECTOR AND CRITICAL INFRASTRUCTURE

The modern power grid has become more exposed to cyber stress conditions from both malicious and unintentional sources. To maintain reliable performance, the rapid evolution of technology makes it imperative to closely reexamine and accurately characterize new cyber-influenced operational thresholds (including grid timing services) needed to maintain the reliable/resilient performance of the Nation's critical energy infrastructure.

The Challenge

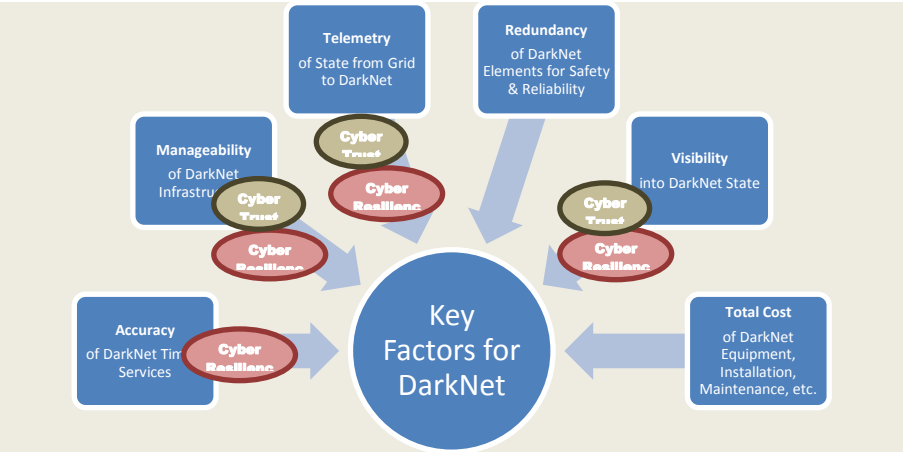
Accurate and synchronized timing signals is critical to safe, reliable, resilient, and secure operation of the Nation's energy infrastructure. Therefore, cyber security is key to making sure that transmission, reception and trustworthiness of these signals and the coordinated communications required to manage them is guarded from intentional (malicious) exploitation and accidental intrusion. Some of these vulnerabilities are relatively well understood (such as natural events like earthquakes) while others are only recently emerging, broadly falling into the category of cyber phenomena.

In particular, two key cyber elements affecting the grid's timing capability are Cyber Resilience and Cyber Trust. Characterization of their effects with respect to performance thresholds and spatiotemporal dynamics is critical towards developing mitigation strategies that achieve and maintain operational performance in the presence of cyber stress conditions, including malicious as well as non-intentional occurrences such as malware, misconfiguration, and calibration drift.

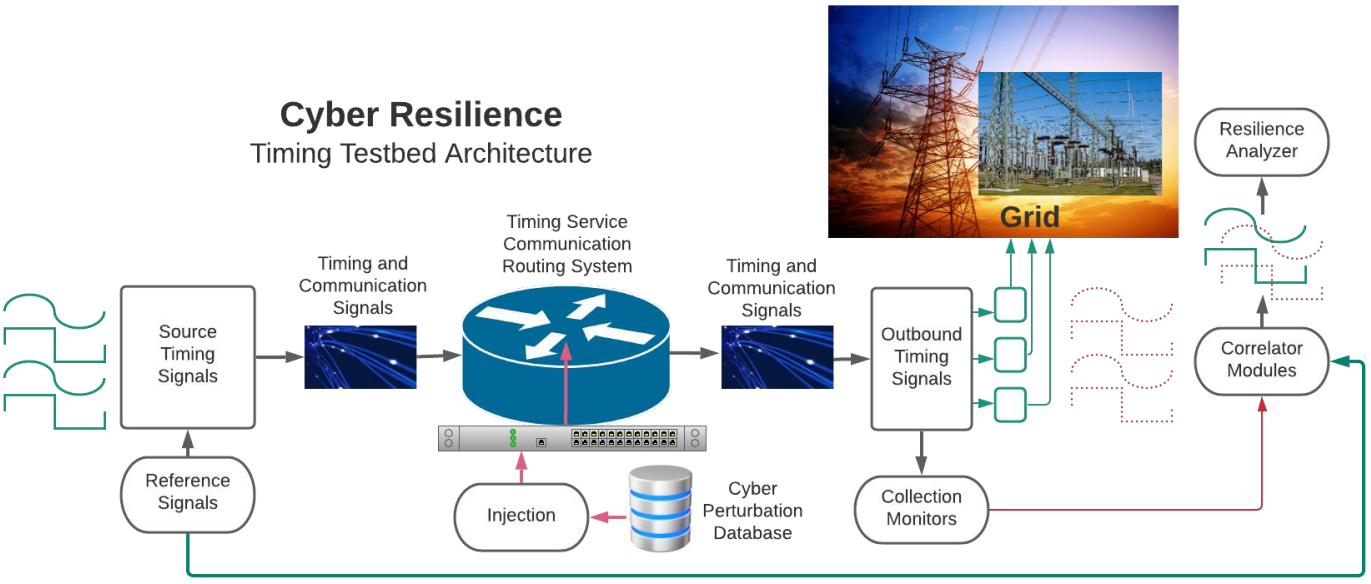
Traditional cyber resilience is concerned with phenomena such as time drift over long periods of time. In contrast, cyber events and perturbations have characteristically atypical impact profiles and effects. As a result, mitigation approaches require different data sets and analyses that simultaneously supplement and complement traditional, non-cyber-specific resilience, reliability, and safety.

The Solution

Grid resilience must now be concerned with preventing, or at least bounding, the limits of perturbations introduced into the timing services of DarkNet by undesirable cyber phenomena. Since perimeter security is insufficient to eliminate all undesirable cyber events, it is important to evaluate a range of intrusive effects that have been recently



Cyber Resilience and Cyber Trust in DarkNet



uncovered in the convergence of operational technology and information technology infrastructures.

Starting with basic functionality, the timing services of DarkNet, will be systematically subjected to a range of cyber phenomena that stress four key performance factors, namely: Accuracy, Manageability, Telemetry, and Visibility (see figure above). This analysis is designed to provide insights into four important categories of undesirable cyber phenomena: Loss of View (LoV), Loss of Control (LoC), Manipulation of View (MoV), and Manipulation of Control (MoC).

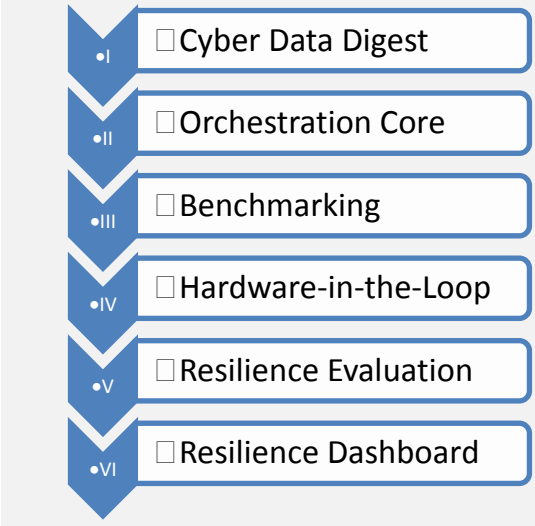
Furthermore, this effort is aimed at an accurate characterization of these effects and their impacts on DarkNet timing infrastructure. The resulting characterization will evolve into a novel catalog that maps cyber stress conditions to verifiable symptoms for the purpose of early detection and recovery operations. This is expected to reduce the time for detection of degraded performance and facilitate quicker recovery operations. Even more importantly, it helps distinguish cyber-induced events from "naturally occurring" grid anomalies (such as weather-related events and mechanical failures) that exhibit similar symptoms but have fundamentally different causes.

The Mission

Ongoing efforts and future research are focused on authentication and trust certificate architectures for DarkNet to evaluate their effects on cyber resilience. Of particular interest is evaluating the resilience characteristics of novel solutions based on distributed ledger technology (DLT), blockchain, and quantum key distribution (QKD). The scaling effects of these solutions on core timing services are largely unknown and warrant further investigation.

Furthermore, as penetration of renewable and distributed energy sources increases in the grid, and traditional energy technologies evolve, alternative timing sources are becoming more appealing as solutions to improve grid redundancy and reliability. In this context, the cyber resilience of alternative timing sources becomes highly relevant. Re-characterizing and understanding their performance thresholds under varying cyber stress conditions is an important aspect to explore. This research will help discover the thresholds for artificial sources of timing relative to GPS-bases solutions.

The insights and findings from these DarkNet developments are envisioned to broadly influence the next generation of technology innovation to holistically account for the cyber resilience and trust dimensions in fundamental design of grid



Cyber Resilience Evaluation Components

Kalyan Perumalla and Juan Lopez, Oak Ridge National Laboratory

OAK RIDGE National Laboratory