Performance, Robustness, and Cyber Security of Critical Infrastructure Systems – A Cyber-Physical Systems Research Theme

Background

Critical infrastructures are complex physical and cyber-based systems that form the lifeline of modern society, and their reliable and secure operation is of paramount importance to national security and economic vitality. The US President's Commission on Critical Infrastructure Protection (CCIP) [1] has identified telecommunications, electric power systems, natural gas and oil, banking and finance, transportation, water supply systems, government services, and emergency services, as the eight critical infrastructure systems. These infrastructures are not only complex and intertwined with electric power and cyber systems, but are highly interdependent among themselves and hence a disruption in one infrastructure will have cascading effects on others [1, 2]. The disruption could be due to natural events, such as hurricanes, earth quakes, and wild fires or due to man-made malicious events, such as physical destructions or electronic intrusions into infrastructure systems. Identifying, understanding, and analyzing such interdependencies among infrastructure systems pose significant challenges [2-4]. These challenges are greatly magnified by the geographical expanse and complexity of individual infrastructures and the nature of coupling among them. The rest of the discussion focuses on electric power infrastructure.

The electric power grid, as of today, is a highly automated network. A variety of communication networks are interconnected to the electric grid for the purpose of sensing, monitoring, and control. These communication networks are closely associated with the supervisory control and data acquisition (SCADA) systems in the network. The data provided by the SCADA system is utilized in the energy management systems (EMS) of the power grid, for a wide range of system operation functions and real-time control of the power grid. Currently, the electric power infrastructure does not have adequate measures to guarantee protection against many forms of natural and malicious physical events on the infrastructure, which makes it highly vulnerable [3-6]. One of the primary concerns has been the issue of large-scale fault events and their impact on the overall performance and stability of the electric grid. Various incidents in the recent past [3-5] have indicated the extent to which the electric grid is vulnerable and the urgent need to protect them against physical and electronic faults and intrusions.

Theme 1: Performance and Robustness of Critical Infrastructure Systems

Research: There is need for fundamental research harnessing the enabling power of sensor networks for real-time monitoring and control of complex dynamical critical infrastructure systems. The goal should be to significantly improve the robustness and performance of the electric energy grid through innovative embedded sensor network design and associated data aggregation, fault diagnosis, and decision algorithms [6].

The overarching goal should be to lay a strong foundation for design and analysis of embedded sensor networks whose optimization/constraints are governed by the underlying dynamics of the physical system. One approach is to deploy sensors in critical and vulnerable locations of the power systems to sense mechanical properties of its various components and transmit the sensed data through a suitable

wireless network to the central control center, and fuse the information with existing data for the electrical quantities in the system to arrive at an ideal preventive or corrective control decision..

Theme 2: Cyber Security of Critical Infrastructure Systems

Three modes of malicious attacks on critical infrastructure are generally envisioned: 1) Attacks upon the system - The system itself is the primary target with ripple effects throughout society, 2) Attacks by the system - The population is the actual target, using parts of the system as a weapon, 3) Attacks through the system - The system provides a conduit for attacks on other critical infrastructures. In some sense, the cyber system forms the backbone of nation's critical infrastructures, which means that a major cyber security incident could have significant impacts on the safe operations of the physical systems that rely on it.

Security threats against utility assets have been recognized for decades [3-5]. Insecure computer systems may lead to catastrophic disruptions, disclosure of sensitive information, and frauds. Cyber threats result from exploitation of cyber system vulnerabilities by users with unauthorized access. A potential cyber threat to supervisory control and data acquisition (SCADA) systems, ranging from computer system to power system aspects, is recognized. It is shown that an attack can be executed within an hour once the computer system security is compromised. The ever increasing power of the Internet facilitates simultaneous attacks from multiple locations. The highest impact of an attack is when an intruder gains access to the supervisory control access of a SCADA system and launches control actions that may cause catastrophic damages. Another primary concern has been the possibility of massive denial of service (DoS) attacks on the SCADA control system and the resulting impacts on the overall performance and stability of the electric power systems.

Research: The overarching research should be to develop a comprehensive cyber security framework for critical infrastructure systems integrating the dynamics of the physical system as well as the dynamics of the cyber-based control network. The integration of cyber-physical attack/defense modeling with physical system simulation capabilities must be developed to quantify the potential damage a cyber attack can cause on the physical system in terms of capacity/load loss, equipment damage, or economic loss in other forms [7]. The integrated model should provide a foundation to design and evaluate effective countermeasures, such as mitigation and resilience algorithms against large scale cyber-based attacks.

Conclusion

These challenging problems call for inter-disciplinary research collaboration between physical as well as cyber systems researchers, and call for laying strong foundation for inter-disciplinary educational program on cyber-enabled critical infrastructure systems focusing on protection, security, resiliency, and sustainability.

References

[1] Presidents Commission on Critical Infrastructure Protection, Critical Foundations: Protecting Americas Infrastructures (1997). [Online]. Available at: http://www.ciao.gov/.

[2] M. Rinaldi, James P. Peerenboom, and Terrence K. Kelly, "Identifying, understanding, and analyzing critical infrastructure dependencies, *IEEE Control Systems Magazine,* pp. 11-25, Dec. 2001.

[3] Control Systems Security Program, US-CERT, Department of Homeland Security. http://www.us-cert.gov/control_systems/

[4] M. Amin, "Security challenges for the electricity infrastructure," *IEEE Security and Privacy Mag.*,

vol. 35, no. 4, pp. 8–10, Apr. 2002.

[5] G. Ericsson, “Toward a framework for managing information security for an electric power utility - CIGR´E experiences,” *IEEE Trans. on Power Delivery,* vol. 22, no. 3, pp. 1461–1469, Jul. 2007.

[6] R. A. Le´on, V. Vittal, and G. Manimaran, “Application of sensor network for secure electric energy infrastructure,” *IEEE Trans. on Power Delivery,* vol. 22, no. 2, pp. 1021–1028, Apr. 2007.

[7] C.-W. Ten, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cyber security for SCADA systems," *IEEE Trans. on Power Systems*, to appear, 2008.

The opinions and positions in the white papers and comments posted on this web site are those of the submitters only and do not necessarily represent those of the Federal government, the NITRD program and its participating agencies, or the National Coordination Office.