Understanding the Resilience of Cyber-Physical Systems Using Complex Networks Theory

Subhash Lakshminarayana*
* School of Engineering, University of Warwick, UK
Emails: *subhash.lakshminarayana@warwick.ac.uk

I. Introduction

Critical infrastructures (e.g., power grids, transportation systems, etc.) are undergoing a fundamental transformation from closed and centrally managed systems to one that integrates distributed players. The integration of massively deployed smart sensing, computing, and network technologies, also known as the industrial internet of things (IIoTs), is improving the capability for monitoring, automation, and control of the physical systems. However, decentralized operation and IIoTs have also opened a door for potential attackers to intrude on the physical system and disrupt their operation. Recent cyber attacks against critical infrastructures, e.g., Stuxnet [1] and BlackEnergy attack [2] are real-world examples of such attacks. Such systems, which involve a cyber network (i.e., the IT infrastructure) closely interacting with a physical infrastructures, and are collectively addressed as cyber-physical systems (CPSes).

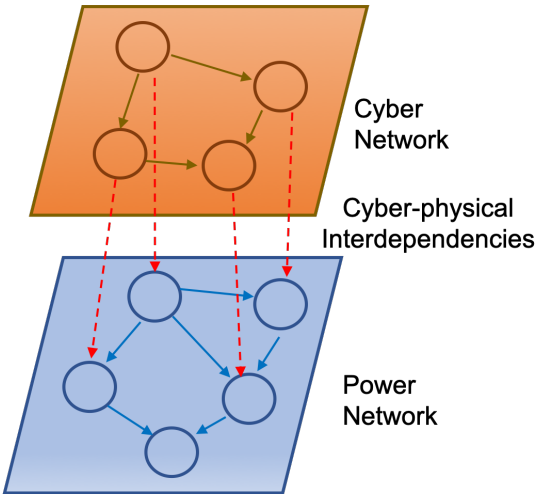

Fig. 1: Cyber-physical systems as a complex network.

II. Proposed Project

The project will consider the potential widespread integration of internet-of-things (IoT) enabled devices at the consumer side (such as Wi-Fi enabled air conditioners, water heaters, etc.). The objective is to present a comprehensive understanding of large-scale IoT-based cyberattacks against the power grid [3]. We will analyze how load altering attacks at a large number of nodes affects the power grid frequency dynamics using tools from control theory and complex network theory. The problem translates to analyzing how large-scale attacks against peripheral nodes the stability of the system's core nodes in a network.

III. Prospective Outcomes

- Investigate how large-scale attacks at the peripheral nodes affects the stability of the system's core nodes.
- Identify cyber and physical interdependencies that are most influential and can potentially degrade the system stability.
- Model collective failure probability based on the interconnections and the coupling dynamics.
- Assess the structural vulnerability of CPSes and design resilient architectures.

References

[1] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security Privacy*, vol. 9, no. 3, pp. 49–51, May 2011.
[2] R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the cyber attack on the Ukrainian power grid: Defense use case," *Electricity Information Sharing and Analysis Center*, Mar. 2016, https://bit.ly/2UY1WNF.
[3] S. Soltan, P. Mittal, and H. V. Poor, "BlackIoT: IoT botnet of high wattage devices can disrupt the power grid," in *Proc. USENIX Security Symposium (USENIX Security 18)*, Baltimore, MD, Aug. 2018, pp. 15–32.