Analysis and Control for Resilient Interdependent Cyberphysical Networks

Today's cyberphysical infrastructural networks share critical interdependencies. Consider the interdependence between communication control networks with the electrical power grid. While these interdependencies are beneficial during normal operation, it can be harmful when the networks are under attack. Indeed, in such multi-layer interdependent cyberphysical networks, a cascade of failures may occur among the various networks following the failure of a small number of nodes in just one network. Failures in one network lead to failures in the other network, and vice-versa, resulting in a significant part of the cyberphysical infrastructure becoming unavailable. For instance, a malware attack may cause a cascade of infections which cripples the communication control infrastructure, leading to cascading power failures, which in turn lead to further communication network failures. Such cascading failures can occur in other interdependent cyberphysical systems, such as sensor-actuator networks, transportation networks, and content distribution networks.

In spite of the significance of the threats facing multi-layer interdependent cyberphysical networks, there are currently substantial holes in our understanding of these networks. There is a great need to develop the analytical foundations for characterizing multi-layer interdependent cyberphysical networks subjected to attacks. To that end, we believe a three-pronged approach is needed: (i) development of analytical models for robustness of interdependent networks, (ii) analysis of interdependent network response to attacks, and (iii) development of dynamic control algorithms to mitigate the effects attacks in multi-layer interdependent networks.

When networks are affected by an attack, a substantial portion of the network links and nodes may be seriously damaged or completely disabled in a spatially and temporally correlated manner. In this situation, it may be too demanding to expect that the remaining network stays fully connected. Rather, we may consider the network to be resilient if it remains largely connected after the attack, a notion that can be made precise using percolation theory, which focuses on the study of connectivity in large-scale networks. We believe this approach should be used to study network resilience to attacks. Specifically, it is important to investigate the conditions for the network to be largely connected, in the presence of concentrated attacks. This network resilience analysis can be leveraged to study the response of multi-layer interdependent networks to attacks.

Based on models for network interdependence, one can design network protection and control techniques for minimizing the impact of attacks in multi-layer and multi-dependent networks. We may take a multi-stage approach that combines survivable network designs, dynamic control algorithms, and network co-recovery techniques. Survivable network designs provide a first line of defense against attacks by utilizing proactive defense techniques including: (i) Resilient topology

design: design network topologies that are robust to concentrated failures and failure cascades. (ii) Cross-layer resource augmentation: develop optimal backup resource allocation schemes over multiple network layers to protect the network from a suspected failure or attack. On the other hand, dynamic control algorithms aim at mitigating the effects of an attack to sustain essential network capabilities. Several approaches can be used to address this problem; including: (i) Control under extreme conditions: network control with imperfect information and stochastic epidemic models can be leveraged to develop stabilizing policies for networks at risk of experiencing cascades. (ii) Load-shedding: in some situations it may be necessary to use load shedding around the periphery of the area affected by the attack, in order to prevent the onset of cascades. There is a need to develop intelligent load shedding strategies. (iii) Islanding: it is important to explore the idea of islanding, where nodes are temporarily disconnected from the part(s) of the network, which is perceived to be experiencing a cascade. This is the networking equivalent of a quarantine, and has the effect of limiting failures and congestion to a small area. Finally, it is worthwhile to investigate efficient network recovery strategies that can coordinate the restoration of multiple interdependent networks for minimizing the aggregated performance loss over space and time.