Building Cyber-Enabled Resilience in Infrastructure Systems

Saurabh Amin, Massachusetts Institute of Technology

Resilience of critical infrastructure systems is a key requirement in the vision of smart cities. These systems work continuously to enable the essential services such as water, gas, and electricity. They utilize diverse components organized as physical networks, and operated through heterogeneous and connected cyber elements. Many service utilities routinely face reliability concerns due to aging infrastructure, and lack the operational readiness that is needed to respond failures caused by natural disasters. Moreover, recent incidents have demonstrated that malicious entities can disrupt or gain control of these systems by exploiting cyber insecurities and/or physical faults. Indeed, sophisticated cyber intrusions and a number of successful physical attacks all confirm the insufficiency of the existing protection solutions. Such incidents can result in huge economic losses, and also pose threat to human lives. Since resiliency was not considered at the design stage of existing infrastructure systems, they continue to face significant risks from natural disasters and security attacks.

This talk is motivated by the need for a foundational approach for strategic security planning and operational response design, so that our infrastructure systems can better withstand, recover from, and adapt to both random and adversarial disruptions. The main agenda is to discuss how recently developed secure and distributed algorithms for network sensing and control can be implemented in practice to improve the resilience of large-scale infrastructure systems. These algorithms use ideas from control theory and large-scale optimization, along with game-theoretic analysis of strategic interaction between network operators and attackers. Through real-world case studies, we demonstrate that our algorithms can provide substantial improvements in strategic inspection and operational response capabilities of electricity and natural gas utilities facing risks of correlated disruptions.

For strategic planning, we show that a small number of secure sensors can significantly improve our understanding of how localized disturbances interact with other and lead to network-level disruptions. This requires developing new physics-based models that capture the impact of dynamic perturbations in individual components (nodes/lines), and evaluating changes in the overall functionality due to network-level effects such as congestion, forced component disconnects and cascading failures. Next, we discuss how these secure sensors can be positioned in the network, possibly in a randomized manner, to detect the presence of strategic adversaries who can simultaneously target and compromise the functionality of multiple components. A key contribution is design of inspection strategies based on the solutions of an attack-defense game.

For operational response design in the aftermath of a natural disaster, we discuss the problem of optimizing the schedules of response crews who face diagnostic uncertainty about the locations of component failures in large-scale network as well as timing and resource constraints. We show that utilizing predictive information on failure events based on infrastructure sensors and customer calls can significantly improve the response operations. We also exploit the structure of the scheduling problem to arrive at scalable and efficient solutions. Finally, we

discuss how strategic allocation of contingency reserves can benefit response and recovery operations in smart distribution grids. We outline an approach to proactively dispatch these reserves to limit the risk of network-level failures (forced outages and cascades) and also reduce the recovery time to nominal operating conditions.