Protecting infrastructure with smarter CPS

September 16 2014, by Eric Brown

Security of IT networks is continually being improved to protect against malicious hackers. Yet when IT networks interface with infrastructures such as water and electric systems to provide monitoring and control capabilities, they often introduce new vulnerabilities that increase the risks of service disruptions.

Considering the potentially catastrophic impacts of coordinated malicious attacks on the power grid and other critical infrastructures, the integration between monitoring networks and infrastructure—called Cyber-Physical Systems (CPS)—has received growing priority as a research focus. The National Science Foundation recently granted $9 million to a five-year Foundations of Resilient Cyber-Physical Systems (FORCES) project involving researchers at MIT, the University of California at Berkeley, Vanderbilt University, and the University of Michigan to help improve CPS technology.

As physical networks are upgraded with sensor and actuation technologies, new services are possible—such as state awareness, real-time monitoring, and active control, which together can improve efficiency and performance. Yet these systems are typically not designed with disturbances in mind, or they only protect against nominal disruptions. This is due in part to the limited visibility and effectiveness of off-the-shelf cyber-security tools in a physical network.

"The problem with infrastructure systems is that they're physical," explains Saurabh Amin, an assistant professor of civil and environmental engineering at MIT and head of the Resilient Infrastructure Networks

Lab. "A water network consists of a flow of water, and a power network consists of a flow of electricity. When they're equipped with sensors and actuators, the IT networks can start to monitor and influence the physical dynamics. But they first need to respect the physical dynamics and real-time properties of the physical networks."

Amin, one of three FORCES team members at MIT along with Hamsa Balakrishnan and Asuman Ozdaglar, focuses on the study of robust monitoring and control for physical networks to protect against malicious attacks. "We are applying new methods of monitoring and control to make sure these systems are robust, efficient, and resilient to attacks," he says. "We try to improve resilience so when bad things happen, the disruption of services is blocked, or at the very least delayed."

IT networks and security software struggles with physical networks that follow the rule of flow physics more than the dictates of a computer. If the cyber and physical networks aren't well calibrated, "bad things can happen, ranging from safety violations to permanently damaged equipment to loss of life," Amin says. "This coupling makes cyber-physical security of infrastructures more challenging, but also more exciting."

Amin and the FORCES project are focusing on improving security and resilience for electric power, transportation, and water infrastructures. They're also studying a new type of physical network that is only now being designed: smart roads.

"The questions surrounding self-driving cars and smart roads are really CPS questions," Amin says. "How will cars communicate with each other? Can they share road space with human drivers? Will they communicate through roadside infrastructure? And how do we provide the incentives to make these technologies secure enough to avoid incidents?"

A faster, smarter response to attacks

On a physical network, it's often difficult to know the cause of a failure in real time, Amin explains. "The immediate challenge is to locate the problem and prevent the effects from propagating," he says. "You can then start looking for the cause, but it's sometimes hard to tell the difference between a malicious attack and a random fault, such as a failure due to wear and tear. We have to design the algorithms for diagnostics, monitoring, and control so they can react quickly to multiple causes."

If a malicious hacker or disgruntled employee gains unauthorized access to the network, "They can play with the data affecting physical dynamics," Amin says. "They can bypass fault-tolerant and secure mechanisms and modify data for sensing and actuation. Such attacks can cause leaks and bursts in water networks, or localized and even cascading failures in electricity networks."

Another attack technique is to jam communications between critical nodes so that information scheduled to arrive in two milliseconds takes two minutes, or never arrives at all. "If the critical decision-making points are missed, the loss of availability of information can result in a loss of stability and safety," Amin says.

Network security tools, such as intrusion-detection and prevention systems that scan for malicious behaviors based on known data signatures and patterns, are typically unprepared for CPS. To address this gap, Amin is developing model-based diagnostic tools that "integrate the physics of physical systems with the network detection systems," he explains.

The behavior of the physical dynamics during failures is often well known. For example, a water-system operator responding to a pipe burst knows the water flow will likely affect the surrounding pipes in a certain pattern. If an electricity system is compromised, operators usually know which fault-protection devices and generators need to be activated.

Yet this knowledge is typically not integrated into the networking software. "If we can encapsulate this knowledge into models, we are able to do pattern-matching and respond long before the failures happen," Amin says.

Amin's control algorithms can use sensor input to detect if the physical system is the normal, preventive, or emergency mode of operation. He's also attempting to make the algorithms adaptable, so the system can reconfigure the priorities depending on the situation. "In the normal mode, the object is usually to reduce operating cost or maximize efficiency," Amin says. "In preventive mode, it may be a good idea to instead focus on safety."

The algorithms can also enable automatic responses. In an electric network, for example, one might want to automatically activate equipment such as detection devices, circuit breakers, and sectionalizers. "These are normally set for failsafe fault tolerance for natural events, but are not designed for security attacks," Amin says. "So I pull out the results from these mechanisms and design control methods that can respond in time to limit the impact of failures."

CPS-coupled sensors and actuators may improve the monitoring of physical networks, but they can also enable new points of vulnerability, Amin says. For example, smart-grid devices can be potential targets for attackers. "Advanced metering infrastructure devices often have vulnerabilities that can be exploited to affect the physical network," Amin says. "Many of these devices are sunken, so if security is not implemented in the design, it is difficult to do patchwork later on."

Incentive mechanisms and game theory

Amin and the FORCES project are looking beyond CPS technology to also study regulatory and business implementation issues. The key challenge is that infrastructure operators often lack incentives to invest in resilient CPS systems.

In a few cases, a business case is clear. Although Amin's main focus is protecting against malicious hackers intent on crippling infrastructure, the new CPS tools may also help power utilities protect against lower levels of smart-grid crime. For example, the algorithms could potentially identify consumers who are stealing electricity, or detect when local producers with rooftop solar panels overreport the amount of energy they're selling back to the grid, Amin says.

Yet such power theft is so far a modest threat, and typically, utilities have even less incentive to act. "If there is no external imposition or oversight, private entities often won't invest in security and reliability," Amin says. "Government regulators can create incentives by imposing taxes, fines, and penalties, or insist on greater monitoring. They can also offer reward or subsidies for compliance."

Such incentive mechanisms are complicated by the differing needs and objectives of stakeholders, including operators, IT firms, service providers, and users. "Our challenge to find out how to incentivize all these activities for the public good," Amin says.

To understand complex networks that involve multiple stakeholders and potentially multiple independent attackers, Amin turns to game theory. "When there is one or more attackers and one or more defenders, game theory can help us better understand the behavior of each," Amin says.

"We model what one player knows about other players, and what they can do to affect the other players' objectives."

The recent study of the interplay between incentives and diagnostic methods and control algorithms is an important one, Amin says. "If the incentives and the actions of human decision-makers are not taken into account, the effectiveness of control algorithms is lessened," he says. "The human decision-makers need to realize the benefits of the diagnostic and control mechanisms, and these mechanisms also need to take into account likely responses of the human decision-makers while implementing autonomous actions."

This story is republished courtesy of MIT News (web.mit.edu/newsoffice/), a popular site that covers news about MIT research, innovation and teaching.

Provided by Massachusetts Institute of Technology

Citation: Protecting infrastructure with smarter CPS (2014, September 16) retrieved 20 March 2024 from https://phys.org/news/2014-09-infrastructure-smarter-cps.html