New software spots, isolates cyber-attacks to protect networked control systems

May 14 2013, by Matt Shipman

(Phys.org) —Researchers from North Carolina State University have developed a software algorithm that detects and isolates cyber-attacks on networked control systems – which are used to coordinate transportation, power and other infrastructure across the United States.

Networked control systems are essentially pathways that connect and coordinate activities between computers and physical devices. For example, the systems that connect temperature sensors, heating systems and user controls in modern buildings are networked control systems.

But, on a much larger scale, these systems are also becoming increasingly important to national infrastructure, such as transportation and power. And, because they often rely on wireless or Internet connections, these systems are vulnerable to cyber-attacks. "Flame" and "Stuxnet" are examples of costly, high-profile attacks on networked control systems in recent years.

As networked control systems have grown increasingly large and complex, system designers have moved away from having system devices – or "agents" – coordinate their activities through a single, centralized computer hub, or brain. Instead, designers have created "distributed network control systems" (D-NCSs) that allow all of the system agents to work together, like a bunch of mini-brains, to coordinate their activities. This allows the systems to operate more efficiently. And now these distributed systems can also operate more securely.

NC State researchers have developed a software algorithm that can detect when an individual agent in a D-NCS has been compromised by a cyber-attack. The algorithm then isolates the compromised agent, protecting the rest of the system and allowing it to continue functioning normally. This gives D-NCSs resilience and security advantages over systems that rely on a central computer hub, because the centralized design means the entire system would be compromised if the central computer is hacked.

"In addition, our security algorithm can be incorporated directly into the code used to operate existing distributed control systems, with minor modifications," says Dr. Mo-Yuen Chow, a professor of electrical and computer engineering at NC State and co-author of a paper on the work. "It would not require a complete overhaul of existing systems."

"We have demonstrated that the system works, and are now moving forward with additional testing under various cyber-attack scenarios to optimize the algorithm's detection rate and system performance," says Wente Zeng, a Ph.D. student at NC State and lead author of the paper.

More information: The paper, "Convergence and Recovery Analysis of the Secure Distributed Control Methodology for D-NCS," will be presented at the IEEE International Symposium on Industrial Electronics, May 28-31, in Taipei, Taiwan.

Abstract
Distributed control algorithms (e.g., consensus algorithm) are vulnerable to the misbehaving agent compromised by the cyber-attacks in Distributed Networked Control Systems (D-NCS). In this paper we continue our work on the proposed secure distributed control methodology that is capable of performing a secure consensus computation in D-NCS in the presence of misbehaving agents. The methodology is introduced first and proved to be effective through the

convergence analysis. We then extend our secure distributed control methodology to the leaderless consensus network by introducing and adding two recovery schemes into the current secure distributed control framework to guarantee the accurate convergence in the presence of misbehaving agents. All phases in our method are distributed in the sense that at each step of the detection, mitigation, identification, update and recovery, every agent only uses local and one-hop neighbors' information. The simulation results are presented to demonstrate the effectiveness of the proposed methods.

Provided by North Carolina State University