Cutting off stealthy interlopers: A framework for secure cyber-physical systems

March 4 2021, by Nari Kim

Credit: AI-generated image (disclaimer)

Cyber-physical systems (CPS), which combine modern networking with physical actuators, can be vulnerable against hackers. Recently, researchers at DGIST developed a new framework for CPSs that is resilient to a sophisticated kind of cyberattack. Unlike existing solutions, the proposed approach allows for real-time detection and recovery from

the attack while ensuring stable operation. This paves the way for secure and reliable CPSs across various application domains, such as smart cities and unmanned public transportation.

In 2015, hackers infiltrated the corporate network of Ukraine's power grid and injected malicious software, which caused a massive power outage. Such cyberattacks, along with the dangers to society that they represent, could become more common as the number of cyber-physical systems (CPS) increases.

A CPS is any system controlled by a network involving physical elements that tangibly interact with the material world. CPSs are incredibly common in industries, especially those integrating robotics or similar automated machinery to the production line. However, as CPSs make their way into societal infrastructures such as public transport and energy management, it becomes even more important to be able to efficiently fend off various types of cyberattacks.

In a recent study published in *IEEE Transactions on Industrial Informatics*, researchers from Daegu Gyeongbuk Institute of Science and Technology (DGIST), Korea, have developed a framework for CPSs that is resilient against a sophisticated kind of cyberattack: the pole-dynamics attack (PDA). In a PDA, the hacker connects to a node in the network of the CPS and injects false sensor data. Without proper readings from the sensors of the physical elements of the system, the control signals sent by the control algorithm to the physical actuators are incorrect, causing them to malfunction and behave in unexpected, potentially dangerous ways.

To address PDAs, the researchers adopted a technique known as software-defined networking (SDN), whereby the network of the CPS is made more dynamic by distributing the relaying of signals through controllable SDN switches. In addition, the proposed approach relies on

a novel attack-detection algorithm embedded in the SDN switches, which can raise an alarm to the centralized network manager if false sensor data are being injected.

Once the network manager is notified, it not only cuts the cyberattacker off by pruning the compromised nodes but also establishes a new safe path for the sensor data. "Existing studies have only focused on attack detection, but they fail to consider the implications of detection and recovery in real time," explains Professor Kyung-Joon Park, who led the study, "In our study, we simultaneously considered these factors to understand their effects on real-time performance and guarantee stable CPS operation."

The new framework was validated experimentally in a dedicated testbed, showing promising results. Excited about the outcomes of the study, Park remarks, "Considering CPSs are a key technology of smart cities and unmanned transport systems, we expect our research will be crucial to provide reliability and resiliency to CPSs in various application domains." Having a system that is robust against cyberattacks means that economic losses and personal injuries can be minimized. Therefore, this study paves the way to a more secure future for both CPSs and ourselves.

More information: Sangjun Kim et al. Stealthy Sensor Attack Detection and Real-Time Performance Recovery for Resilient CPS, *IEEE Transactions on Industrial Informatics* (2021). DOI: 10.1109/TII.2021.3052182

Provided by Daegu Gyeongbuk Institute of Science and Technology

March 4) retrieved 3 May 2024 from https://techxplore.com/news/2021-03-stealthy-interlopers-framework-cyber-physical.html