New control architecture defends complex interconnected systems against cyberattacks

October 26 2020

Credit: CC0 Public Domain

Researchers have developed a novel control architecture that defends complex, interconnected systems previously vulnerable to cyberattacks. Details were published in *IEEE/CAA Journal of Automatica Sinica*.

Distributed systems are becoming more and more essential in everyday life. From power plants to autonomous vehicles, modular, interconnected systems, colloquially referred to as cyber-physical systems (CPS), provide crucial services and capabilities while being technologically cost effective.

While well-suited for many applications, these architectures are particularly vulnerable to cyberattacks. These systems typically operate via an open communication structure, allowing the individual components to rapidly communicate with each other in order to maintain stability and precise control. Due to the nature of this network topology and the frequent connections necessary for optimal operation, CPS are particularly vulnerable to denial of service (DoS) attacks. DoS attacks can infect a portion of a CPS and through the open communication structure subsequently cascade through the entire system, degrading overall performance and even causing total failure.

Through clever implementation of a set theory-based, novel control paradigm, researchers from Italy and Canada have found a way to mitigate these particularly damaging cyberattacks by implementing a Leader-Follower approach. This approach uses one portion of the network to manage communications to the rest of the network. By assigning different roles to different portions of a CPS, the team was able to design an algorithm that can detect when and where a DoS attack occurs in the network. Upon detection, the algorithm is then able to cut off the infected portion of the network to prevent large-scale degradation while also dynamically adapting to the now-modified network structure. The algorithm can even assign new roles to different portions of the network in response to infection, increasing the robustness of the system against targeted DoS attacks.

"Organizing the distributed controllers in a Leader-Follower paradigm allows us to reduce the data exchange and provide the entire system with

a modular capability so that it is possible to disconnect the attacked sub-subsystems without affecting the global operations" said Dr. Francesco Tedesco of the University of Calabria, corresponding author of the study. "Therefore, the success chance of the adversary attack can be significantly mitigated."

Tedesco goes on to say that the algorithm is not only secure; it is computationally efficient. "The required computational resources —CPUs power, memory resources and bandwidth requirements—are modest which clearly leads to a low economic impact."

As for what's next, the team is working to detect and apply more specific actions to counter cyberattacks based on predictive ideas, decreasing response time and further dampening the undesirable cascading effect of cyberattacks against interconnected systems.

More information: Giuseppe Franze et al. A resilient control strategy for cyber-physical systems subject to denial of service attacks: A leader-follower set-theoretic approach, *IEEE/CAA Journal of Automatica Sinica* (2020). DOI: 10.1109/JAS.2020.1003189

Provided by Chinese Association of Automation