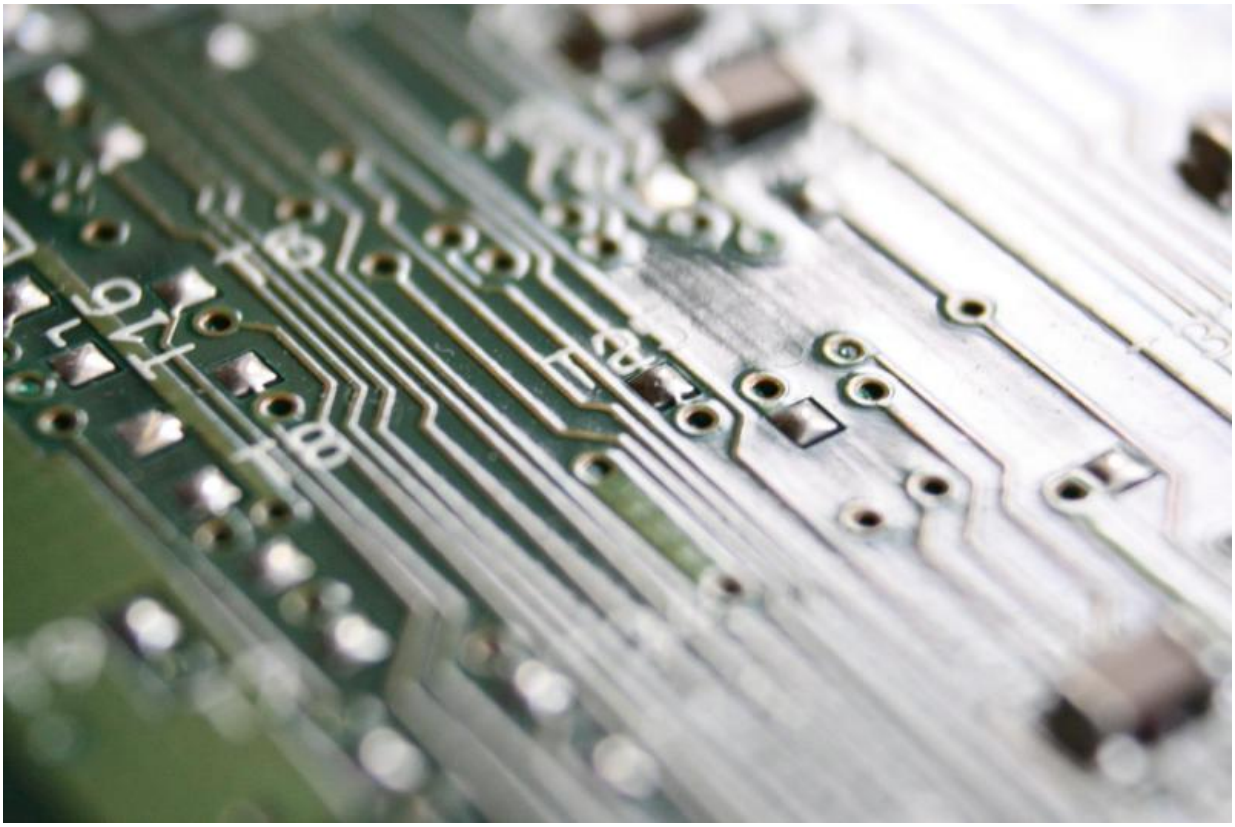
Resilience against replay attacks in computer systems

April 12 2021



Credit: Public Domain

From power grids and telecommunications to water supply and financial systems, digital data controls the infrastructure systems on which society relies. These complex, multi-tier systems depend on layered

communications to accomplish their tasks—yet every point of contact becomes a potential target, every path of information a potential weak spot for malicious actors to attack.

A team of researchers from the University of Calabria in Italy has developed the first predictive control scheme that can help distributed networks with multiple agents not only identify these attacks but also protect against them. Their approach was published in *IEEE/CAA Journal of Automatica Sinica* (Volume 8, Issue 3, March 2021).

"Modern systems have an increasing complex structure due to the large number of interacting agents aligned to accomplish specific tasks in a distributed fashion," said paper author Giuseppe Franzè, associate professor of control engineering in the Department of Informatics, Modeling, Electronics and System Engineering, University of Calabria. "The key result of the paper is that model predictive control strategies, properly adapted to multi-agent configurations, can address difficult scenarios such as the presence of intrusions such as replay attacks."

Replay attacks are difficult to identify because the malicious actor uses information already in the system. By stealing an account number or a permission string stolen from one transmission and using it on another agent—or even the agent who originally received the transmission—the actor can gain access or incite a specific action.

Franzè and his team applied a "receding horizon" model, that allows the researchers to predict what the system will look like in the future. By understanding what the system should look like, the model can identify when something unexpected occurs, like the resending of information.

"The receding horizon property allows us to consider the same structure of the optimization at each next time instant," Franzè said. "This means that if a problem is solvable at the initial time instant the same occurs in

the future."

Importantly, according to Franzè, the strategy also offers protection by allowing the system to encapsulate in the moment before the attack, preserving communications until the attack can be successfully blocked.

"This low-demand model predictive control scheme is an efficient way to address unknown scenarios where external malicious agents affect normal system operations," Franzè said.

More information: Giuseppe Franze et al. Resilience Against Replay Attacks: A Distributed Model Predictive Control Scheme for Networked Multi-Agent Systems, *IEEE/CAA Journal of Automatica Sinica* (2020). DOI: 10.1109/JAS.2020.1003542

Provided by Chinese Association of Automation