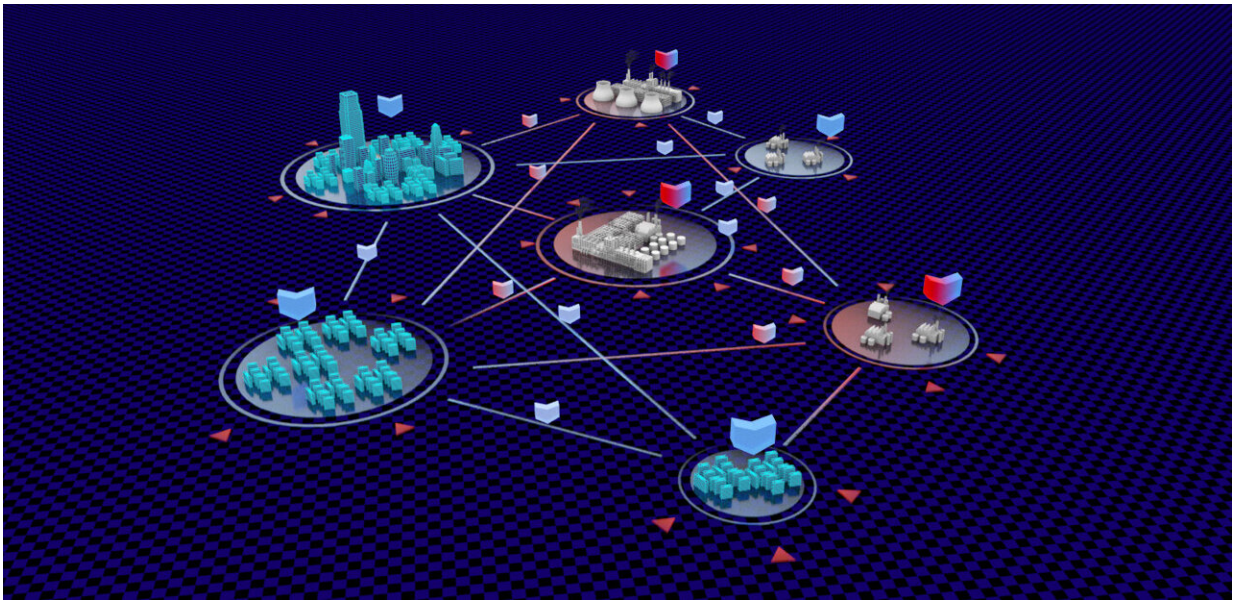
Creating deeper defense against cyber attacks

November 23 2021



Industrial control systems that are widely used to monitor and operate factories and critical infrastructure have largely moved online, making them more vulnerable to cyberattacks. Credit: 2021 KAUST; Heno Hwang

To address the growing threat of cyberattacks on industrial control systems, a KAUST team including Fouzi Harrou, Wu Wang and led by Ying Sun has developed an improved method for detecting malicious intrusions.

Internet-based industrial control systems are widely used to monitor and

operate factories and critical infrastructure. In the past, these systems relied on expensive dedicated networks; however, moving them online has made them cheaper and easier to access. But it has also made them more vulnerable to attack, a danger that is growing alongside the increasing adoption of internet of things (IoT) technology.

Conventional security solutions such as firewalls and antivirus software are not appropriate for protecting industrial control systems because of their distinct specifications. Their sheer complexity also makes it hard for even the best algorithms to pick out abnormal occurrences that might spell invasion.

For instance, system behavior that looks suspicious, such as a freak power surge or the serial failure of circuit breakers, may have natural causes. To add to this, sophisticated cyber attackers may be very good at disguising their movements.

Where algorithms have failed in the past, a branch of machine learning, called deep learning, has proven much more adept at recognizing complex patterns of the kind described above.

Deep learning runs on circuits called neural networks and is trained rather than programed. Instead of writing coded instructions, its creators show the deep learning model different examples to learn from, allowing it to improve in accuracy with every step.

Ying Sun's team trained and tested five different deep learning models with data supplied by the Mississippi State University's Critical Infrastructure Protection Center. These were publicly available simulations of different kinds of attack, such as packet injection and distributed denial of service (DDOS), on power systems and gas pipelines.

The deep learning models' ability to detect intrusions was compared to state-of-the-art algorithms. While the best algorithms were typically between 80 and 90 percent accurate, each deep learning model scored between 97 and 99 percent.

Crucially, when all five deep learning models were "stacked," the accuracy went up to well over 99 percent. Simply put, stacking means adding the results of all five models and taking their average. "We tried stacking two models, then three and four, until five gave us the accuracy we wanted," says Harrou.

The team's stacked deep learning method promises an effective defense in cyberwarfare, which national governments today identify as a major security threat. Cyberattacks such as that on Ukraine's electricity grid in 2015, which led to outages in thousands of homes, may be prevented.

The research was published in *Cluster Computing*.

More information: Wu Wang et al, A stacked deep learning approach to cyber-attacks detection in industrial systems: application to power system and gas pipeline systems, *Cluster Computing* (2021). DOI: 10.1007/s10586-021-03426-w

Provided by King Abdullah University of Science and Technology