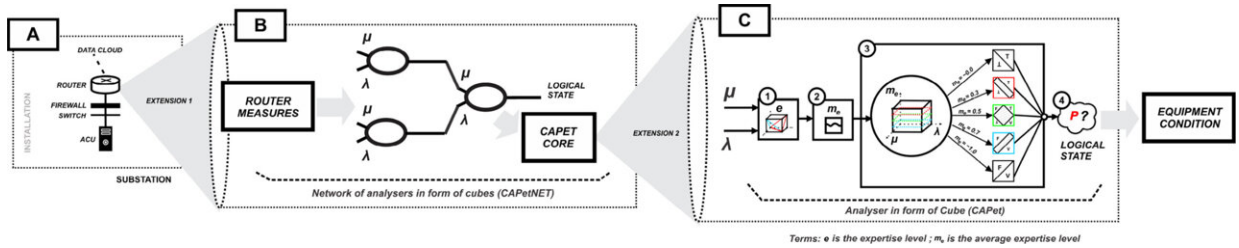
AI can help protect vital networks, say experts

July 3 2023



Credit: *Expert Systems with Applications* (2023). DOI: 10.1016/j.eswa.2023.120536

International experts in artificial intelligence have proposed using AI to help protect critical infrastructure including power, water and communication networks.

The Flinders University and Brazilian experts have worked on a new model to provide early identification of software virus attack, hacker activity or general system failure in vital networks millions of people rely on every day.

"We have developed a novel algorithm to detect failure in data networks that is robust to inconsistencies in the sensor data. This algorithm is capable to signal the start of major disruptions, that could have far-reaching consequences," says Dr. Paulo Santos, Associate Professor in

Artificial Intelligence and Robotics at the College of Science and Engineering at Flinders University.

"This could be advanced to be an effective safeguard against equipment failures in data networks of electrical systems and could replace more traditional diagnostic methods both in power and other critical infrastructure.

"It is one of the first complete investigation of this system of testing paraconsistent analyzers in a large simulation of a complex electrical system."

One example of a critical systems breach, in 2010, was the Stuxnet worm attack, designed to target and disrupt industrial control systems—particularly those used in Iran's nuclear program.

Associate Professor Santos, with co-authors Hyghor Miranda Côrtes from Centro Universitário da FEI, and João Inácio da Silva Filho from Universidade Santa Cecília Brazil, have published their findings in a new article in the journal *Expert Systems with Applications*.

The researchers say that AI can be used to improve software applications and other fault diagnostic systems that help prevent errors in complex engineering systems, or manufacturing plants, and other critical infrastructure.

Already data analysis, machine learning and rule-based learning are used to develop fault diagnostic systems.

"However, we have expanded on these approaches to add an 'evidence filter' to the process of system diagnostics to take into account conflicting evidence by considering a degree of trust in the sensor data," says Associate Professor Santos.

"With further development, this new model of analysis, which we call 'Cubic Paraconsistent Analyser with Evidence Filter and Temporal Analysis' (or CPAet), could be consolidated to address ever more sophisticated technological failures in critical systems which support major industries, entire urban networks, and so on."

More information: Hyghor Miranda Côrtes et al, Cubic Paraconsistent Analysers with Evidence Filter and Temporal Analysis, *Expert Systems with Applications* (2023). DOI: 10.1016/j.eswa.2023.120536

Provided by Flinders University