Detecting and mitigating network attacks with a multi-prong approach

January 16 2020

Credit: CC0 Public Domain

To solve a problem, you must first see the problem. More than that, whatever fallout the problem is causing must be controlled while you solve it. That's the approach an international team of researchers has

taken for combating network attacks. They have published their results in *IEEE/CAA Journal of Automatica Sinica*.

"The communication network and the physical system in a networked control system are vulnerable to potential malicious attacks—including jamming, replay and others," said Dr. Chandreyee Bhowmick, Department of Electrical and Computer Engineering at the Missouri University of Science and Technology.

"One common attribute of all these attacks is that they all tend to deviate the traffic flow in the communications links from the normal value, thus increasing network-induced delays and packet losses."

Bhowmick and colleagues developed a hybrid learning approach to not only detect attacks, but to compensate for the issues the attacks cause. According to Bhowmick, many cyberattacks target information availability rather than data secrecy.

"For such attacks, even the most complicated encryption algorithms fail," Bhowmick said. "To address this issue, in this study, we developed novel attack detection and estimation schemes by using a learning approach that captures the vulnerable communication links, which is challenging because the state matrix is unknown."

The state matrix is the state of the system, which includes the speed and type of information flow. A system under attack has even more unpredictable information flow, or lack thereof. In Bhowmick's proposed scheme, an adaptive observer can detect the onset of attacks and learns how the attacks are disrupting the system. This allows the system to react and perform optimally, even under duress.

However, the proposed method isn't perfect, and the researchers plan to fine-tune their approach to operate in even more complicated attacks.

"Although this approach can detect a broad range of t attacks on both the network and the physical system, detection of sophisticated attacks remains the scope of future work," Bhowmick said. "Studying the signature of such attacks and using probabilistic approach to detect them is one of the prospects of future work."

More information: An optimal hybrid learning approach for attack detection in linear networked control systems, ieeexplore.ieee.org/document/8894751

Provided by Chinese Association of Automation