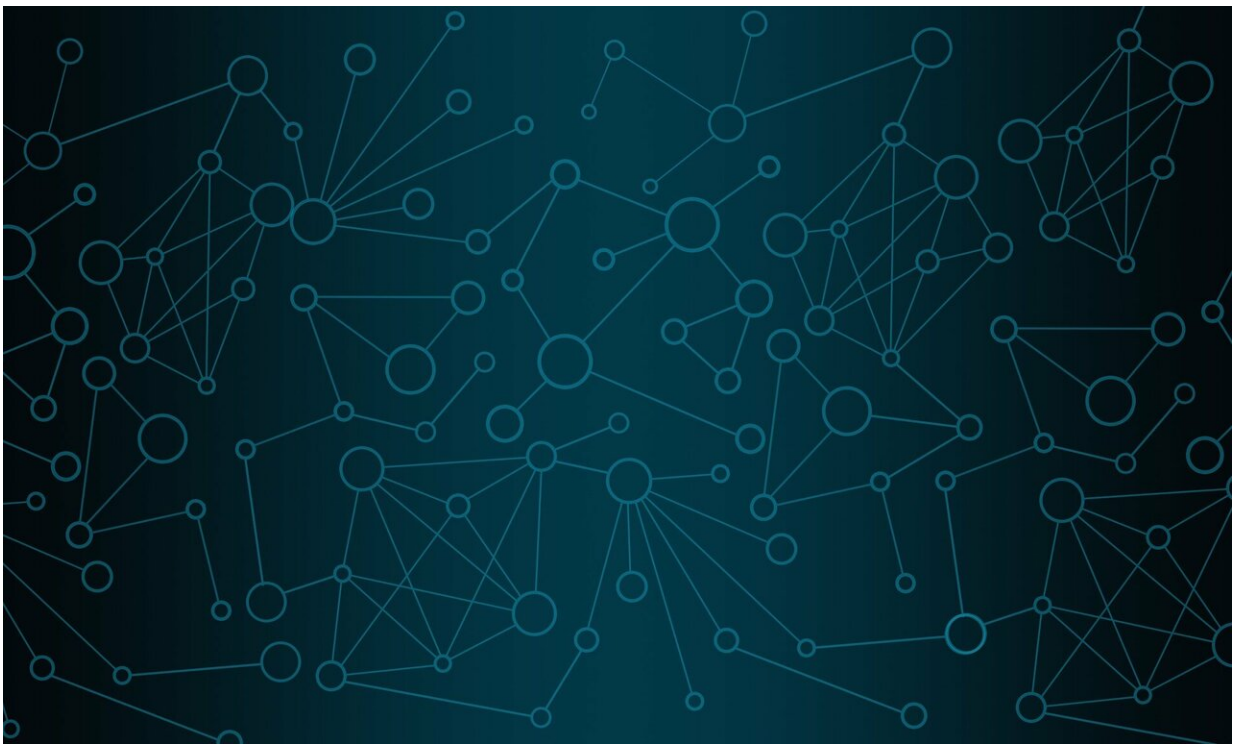
Intrusion alert: System uses machine learning, curiosity-driven 'honeypots' to stop cyberattacks

February 7 2020, by Chris Adam



Credit: CC0 Public Domain

In recent months, the FBI issued a high-impact cybersecurity warning in response to increasing attacks on government targets. Government officials have warned major cities that such hacks are a disturbing trend

that is likely to continue.

A new tool from Purdue University researchers may help stop some of those threats. The Purdue team created a detection system to alert organizations to cyberattacks. The system is called LIDAR—which stands for lifelong, intelligent, diverse, agile and robust.

"The name for this architecture for network security really defines its significant attributes," said Aly El Gamal, an assistant professor of electrical and computer engineering in Purdue's College of Engineering. "Our system is robust and able to adapt to different environments through lifelong learning."

El Gamal created the technology with Arif Ghafoor, a professor in electrical and computer engineering, and Ali Elghariani, a graduate of electrical and computer engineering.

LIDAR can be used for computer systems and networks, including wireless networks. The system works with preprocessing components that are designed to be resilient to adversarial attacks and a cross-layer feature extraction mechanism for wireless networks.

The Purdue system is made up of three main parts: supervised machine learning, unsupervised machine learning and rule-based learning.

"One of the fascinating things about LIDAR is that the rule-based learning component really serves as the brain for the operation," El Gamal said. "That component takes the information from the other two parts and decides the validity of a potential attack and necessary steps to move forward."

The supervised machine-learning component uses an algorithm to compare abnormalities detected in the system to known attack templates.

The unsupervised component uses an algorithm to detect any anomalies in the overall system being monitored.

Purdue's LIDAR system also uses a novel curiosity-driven honeypot, which lures attackers but does not let them infiltrate the system.

Provided by Purdue University