$6 Million Grant for Penn Engineering and CHOP Researchers to Make AI More Resilient to Attacks

Submitted by willirn1 on Wed, 11/25/2020 - 2:46pm

$6 Million Grant for Penn Engineering and CHOP Researchers to Make AI More Resilient to Attacks

November 10, 2020

Volume 67 | Issue 18

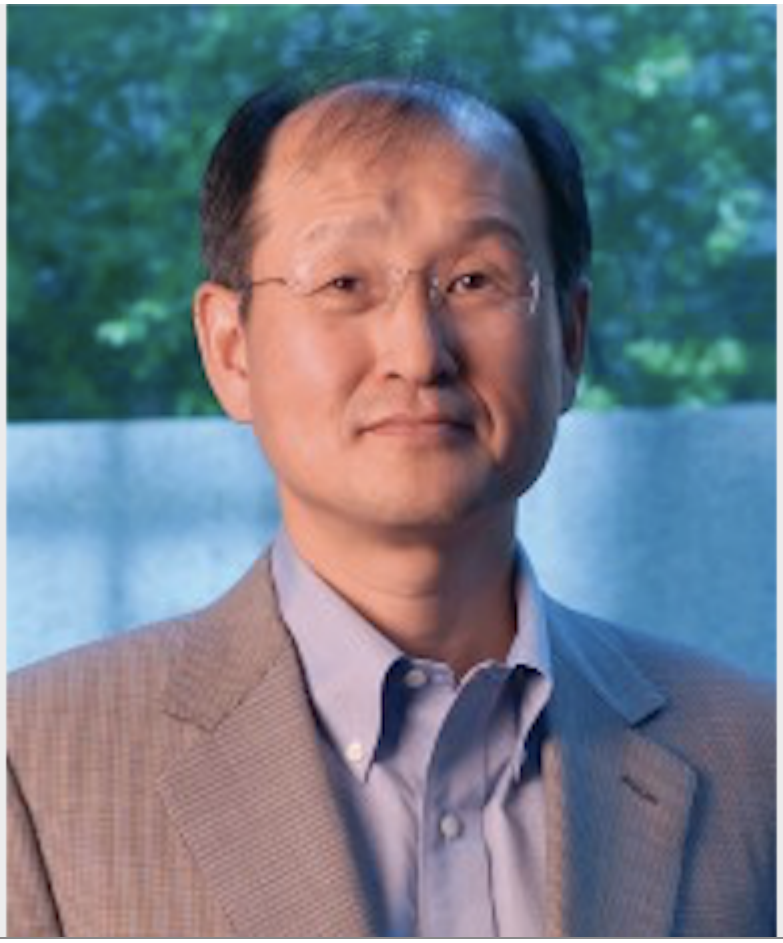
A team of researchers from the University of Pennsylvania's School of Engineering and Applied Science and the Children's Hospital of Pennsylvania (CHOP) have been awarded a five-year, $6 million Multidisciplinary University Research Initiative (MURI) grant. The MURI program is the signature research funding mechanism of the Department of Defense.

The Penn team's proposal, "Robust Concept Learning and Lifelong Adaptation Against Adversarial Attacks," aims to leverage insights from human cognitive development to make artificial intelligence systems better at protecting themselves from malicious disruptions.

With these systems increasingly interacting with the physical world, they are more vulnerable to being confused by ambiguous information. Rather than attempt to directly access the software that controls a self-driving car's accelerator, an ill-intentioned person could subtly alter a speed-limit sign such that the car's AI no longer recognizes it.

By imbuing AI with the kind of robust, adaptive learning capabilities that biological intelligences exhibit, these cyber-physical systems will be able to work with broader categories of information and thus be less prone to potentially dangerous confusion.

Read More Here >>



? National Science Foundation Funds Development of First-of-Its-Kind Drone Cybersecurity Curriculum at Embry-Riddle IEEE Vehicular Technology Magazine June 2020 Special Issue on "Future 5G Networks" & "Unmanned Air Transportation" published! ?

General Announcements