Electrical engineer trains computers to distinguish between friend and foe

College of Engineering
March 2020

University of Arizona electrical and computer engineering assistant professor Gregory Ditzler has received a five-year, $500,000 National Science Foundation Faculty Early Career Development Award to support his machine learning research. The CAREER award is the NSF's most prestigious award in support of exceptional early-career faculty.

"This is about establishing my career moving forward - not just about five years, but how I see things progressing over the next 10 years," Ditzler said. "I can use this opportunity to shape my entire career."

Ditzler's work is all about developing mathematical models and algorithms that computers use to recognize patterns and identify relevant features.

For example, researchers might show a computer a series of electronic medical records taken from patients - some with and some without cancer. Over time, the computer learns to recognize which features are indicative of the disease and which aren't relevant.

"Our goal is to develop a mathematical model the computer can use so if we give it a new item it has never seen before, the machine can infer whether that individual has cancer," Ditzler said. "Machine learning is such a hot topic right now because it's integrated into everything we use in our daily lives - from the computers we use to create Word documents to the cellphones we use to make phone calls, take photos and text."

Machine learning also helps GPS navigation services make traffic predictions, cellphones unlock at the sight of owners' faces, email inboxes recognize spam, and internet bank accounts identify fraudulent activity. With so much personal and financial information living online, it is quickly becoming critical to apply machine learning techniques to cybersecurity.

"Greg's machine learning work is of critical importance in today's world, where all of us rely on digital technology," said Tamal Bose, head of the Department of Electrical and Computer Engineering. "This award is a reflection of Greg's commitment to both research and teaching, which I have witnessed during our collaborations."

With his CAREER Award, Ditzler is tackling two areas of adversarial machine learning and applying his methods and algorithms to cybersecurity. For one, he is examining why feature selection - the process by which a machine decides what elements of information are important to focus on - can fail in the presence of adversaries. An adversary introduces false data into a learning environment to trick a model into misidentifying features.

Autonomous vehicles, for example, use machine learning to learn how to recognize objects around them and react appropriately - like slowing down when approaching another car or..."
stopping at a stop sign. However, researchers have demonstrated that something as simple as placing a sticky note on a stop sign can trick an autonomous vehicle into seeing a speed limit sign instead. Ditzler is investigating what causes this confusion and how it can be prevented.

His work also addresses the problem of machine learning in nonstationary environments. While researchers can develop algorithms that recognize security threats, new forms of threats come up all the time. So, it's critical that these systems be able to learn continuously.

"If you took data from 10 years ago to make a model for investing in the stock market and apply it to today's economy, it wouldn't work," Ditzler explained. "Many algorithms are static. You train them and deploy them, but realistically they have to be able to change over time."

For the educational and community outreach component of the NSF CAREER award, Ditzler is using low-cost robotics to engage Tucson middle school students in science and engineering. He hopes to reach students at an age when many are first starting to think about their career paths.

"This is an opportunity to sit down with students and have them participate in programming and explain that things like autonomous cars are being driven by machine learning and artificial intelligence," Ditzler said.

A version of this article originally appeared on the College of Engineering website.

Source URL: https://uaatwork.arizona.edu/lqp/electrical-engineer-trains-computers-distinguish-between-friend-and-foe

Links
[1] https://ece.engineering.arizona.edu/