Researchers improve security for smart systems

November 8 2022, by Tina Hilding

Credit: Pixabay/CC0 Public Domain

In an increasingly connected and smart world, sensors collect and share large amounts of data to help people make decisions.

Whether it's the smart grid that is continuously monitoring energy usage,

or people trying to track a health condition, people receive ever-increasing amounts of data in ways that can be hard to decipher.

A group of WSU researchers has recently developed a way to statistically analyze such complex sensor data, so that the computer algorithms that make data-based decisions can be more resilient and better able to cope with small errors. The work has applications in many fields, including mobile health, smart homes, the electric power grid, and agriculture. They recently presented their work at the 2022 International Conference on Computer-Aided Design in San Diego.

"This is an important and novel contribution in the area of security of machine learning systems," said Jana Doppa, Huie-Rogers Endowed Chair Associate Professor of Computer Science, who led the work.

Machine learning algorithms are used increasingly for many applications, such as in smart grid management or smart agriculture. So, for instance, they might gather data from sensors in farm fields and weather instruments to learn and predict optimal watering times. The data collected for many smart applications comes in the form of a time-series, which is a data set that tracks a sample over time and provides a sequence of timestamp data points.

Unfortunately, while computers collect information and spew out these time series lines and charts all day, people aren't well suited to easily read and understand them. More importantly, they might miss small but consequential changes—even ones that are done maliciously.

"These types of time-series data are hard to understand by humans," said Taha Belkhouja, a graduate student in the School of Electrical Engineering and Computer Science who has been working on the problem for the past three years. "If we introduce a small perturbation on this sequence of time stamps, then you wouldn't know if we actually

did the perturbation or not and if that reading is correct or not."

As machine learning is being built into more systems, the security of those systems has been an understudied problem, Doppa said. Adversarial attacks can occur when an attacker gains access to smart sensors and then induces small perturbations in the data in a way that wouldn't be noticeable to a person watching the data. The perturbations can lead to a failure of the prediction and decision-making process.

"That's a challenge from an interpretability point of view, which means that it's actually a huge advantage to an adversary who wants to break some of these infrastructures," he said. "You can't notice what is right and what is wrong."

In their work, the WSU researchers introduced a security layer to their machine learning algorithm that looks for potential disturbances and determines how statistically likely they are to happen, providing resilience to the system and preventing major failures. Working with wearable, health monitoring devices, the researchers used their algorithm to automatically account for the real-world sensor data disturbances and improved its accuracy by 50% compared to standard machine learning algorithms which can work with only clean data.

Because the algorithm looks at the statistical likelihood of scenarios, the WSU team also saved computational energy compared to traditional algorithms that have to re-calibrate after the fact. In practical terms, the energy savings would translate to a reduced demand on a device's batteries.

In addition to Belkhouja and Doppa, the researchers on this project included Ganapati Bhat and Yan Yan, assistant professors in the School of Electrical Engineering and Computer Science, and graduate student Dina Hussein.

"Solving this complex problem requires expertise in multiple areas and all the project team members made synergistic contributions," said Doppa.

Provided by Washington State University

Citation: Researchers improve security for smart systems (2022, November 8) retrieved 4 May 2024 from https://techxplore.com/news/2022-11-smart.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.