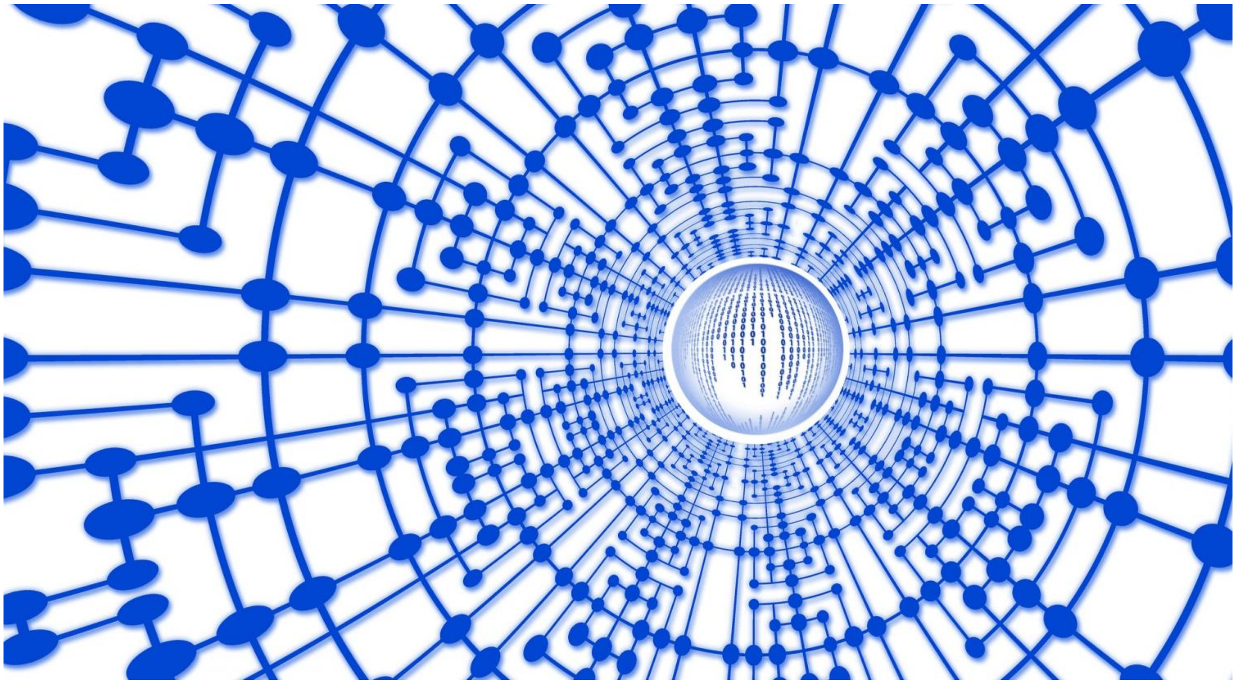
PHYS.ORG

United against jammers: Researchers develop more secure method for data transmission

March 27 2019



Credit: CC0 Public Domain

The motto "united we stand, divided we fall" has found new application in an unlikely discipline—cyber security.

Machines—from simple ones like a personal computer to a complex one like a self-driving car—must transmit information in order to process it. A self-driving car, for instance, is designed to collect the same kinds of information a human driver might, and respond in kind. From traffic lights to the behavior of other cars, the self-driving car must sense and process information quickly and securely in order to decide on a course of action: braking, turning, and potentially saving lives.

But what if there's another, adversarial signal in the mix, jeopardizing the communication? A research team based at the University of Illinois at Urbana-Champaign has developed a method to potentially avoid the interruptions caused by these signals, called jammers.

The research was published in the January issue of *IEEE/CAA Journal of Automatica Sinica (JAS)*, a joint publication of the IEEE and the Chinese Association of Automation.

"The ability to transmit data from a source to a destination reliably in the presence of adversarial intervention, such as jamming, is of paramount importance and concern," said lead author Tamer Basar.

Basar is Swanlund Endowed Chair of the department of electrical and computer engineering and director of the Center for Advanced Study at the University of Illinois at Urbana-Champaign.

"The prototype introduced in the paper captures scenarios that arise in many application areas, such as remote sensing systems, networked control systems, and cyber-physical systems," Basar said.

For example, a sensor collects information over a period of time and transmits the data to a decision center that must work to accurately process the original data. The data can become corrupted as it must be encoded prior to the decision center and decoded afterwards. Time constraints and limited energy resources further complicate matters. To further complicate issues, a jammer can stop everything by literally jamming the system with a gluttony of noise.

"The sensor, the encoder, and the decoder act in unison, toward a common goal, whereas a jammer operates in a way to counteract the actions of the first three," Basar said.

The researchers grouped the three pieces together, comprising one actor in the system, working to counter the actions of the jammer. By having all three pieces work as one, they simultaneously announce their policies regarding information.

It's the difference between communicating via a carrier pigeon or a phone. A person must tie a message to the pigeon's leg, the pigeon must travel, and the receiver must retrieve the message from the pigeon. Then the receiver must respond and repeat the process in reverse. The message could be lost or damaged at several points. If the same people picked up the phone, it's far more likely they could decide on a course of action together with minimal interference.

When the sensor, encoder, and decoder work together, they commit to their next actions together. They don't block the jammer altogether, but the jammer doesn't have the opportunity to interrupt the work and cause a substantial error as the actors communicate back and forth.

Called a Stackelberg feedback solution, this hierarchal maneuver allows the system to commit to processing information based on a set of pre-computable thresholds, which depends on time and the number of transmission opportunities left. The jammer is left out of consideration as the sensor, encoder, and decoder decide together what, how, and when to process.

While effective, the solution is currently limited to one channel. The researchers hope to change that.

"Our goal is to extend the model introduced in the paper to more complex systems, allowing for more general source processes, multiple sensors, multiple channels, and sensors that are equipped with an energy harvester that has the potential to replenish the sensor's used energy based on random availability of such resources—such as solar or wind power," Basar said.

More information: Xiaobin Gao et al, Communication scheduling and remote estimation with adversarial intervention, *IEEE/CAA Journal of Automatica Sinica* (2019). DOI: 10.1109/JAS.2019.1911318

Provided by Chinese Association of Automation

Citation: United against jammers: Researchers develop more secure method for data transmission (2019, March 27) retrieved 27 April 2024 from https://phys.org/news/2019-03-jammers-method-transmission.html