Coding for uncertainty increases security

21 February 2020, by Leah Burrows

Credit: CC0 Public Domain

Right now, drones are flying over wildlife parks in South Africa, equipped with thermal infrared cameras and smart automatic detection systems that can identify potential poachers. If a poacher is spotted, the drone can alert nearby rangers and flash its lights to send up an alarm.

But parks are big places and rangers are spread thin. What if rangers don't always swoop in in response to those flashing lights? Can the technique still deter poachers, like an empty police car in a speed trap? If so, how often can the ploy be used before the poachers get wise?

That is the central question in a new paper from computer scientists at the Harvard John A. Paulson School of Engineering and Applied Sciences (SEAS).

"Our goal was to develop an algorithm that can employ this approach strategically," said Elizabeth Bondi, a graduate student at SEAS and first author of the paper. "We wanted to design a signaling scheme that could mislead a poacher and make them uncertain as to whether they have been detected."

The key, it turns out, was acknowledging the fallibility of the drone itself.

While drones are an important tool to protect wildlife and forests, they aren't perfect. An occluded camera or a misidentified human can lead to false negatives.

By taking these uncertainties into account, Bondi and the team developed an algorithm that could strategically signal in order to trick poachers into believing that rangers could be on their way at any time.

With this algorithm, if a drone sees a poacher and a ranger is nearby, it will sometimes signal because the poacher is likely to be caught. But, if the drone sees a poacher and a ranger isn't nearby, it may signal or it may not, depending on calculations from the algorithm. And, to account for the uncertainty of the device, the drone may signal even if it sees nothing at all.

This acknowledgement of uncertainty gave the algorithm, called GUARDSS, an edge over other strategies. In fact, the researchers found that if a signaling algorithm ignored its uncertainties, it did worse than using no drones at all.

"This algorithm gives us an informational advantage over the poachers," said Bondi. "We know whether or not we've seen them but the poachers don't. We've turned our uncertainties into our advantage."

"Exploiting uncertainties and informational advantages to deceive has long been used by human beings in competitive interactions," said Haifeng Xu, a former postdoctoral fellow at SEAS and co-author of the paper. "It's exciting to discover that such bluffing tactics can also be rigorously computed and implemented as algorithms for the purpose of social good, like to combat illegal poaching."

"This tool can assist rangers in their mission by exploiting real-time information about poaching,"

said Milind Tambe, the Gordon McKay Professor of Computer Science at SEAS and senior author of the paper. "It joins other AI tools we've been building over the past several years to assist rangers and wildlife conservation agencies, including WWF and WCS, in their extremely important work in protecting endangered wildlife."

This research was co-authored by Hoon Oh, Haifeng Xu, Fei Fang and Bistra Dilkina. It was presented at the Association for the Advancement of Artificial Intelligence (AAAI) Conference.

More information: To Signal or Not To Signal: Exploiting Uncertain Real-Time Information in Signaling Games for Security and Sustainability pdfs.semanticscholar.org/6c13/ … 531c1ce6e8d9d22d.pdf

Provided by Harvard University

APA citation: Coding for uncertainty increases security (2020, February 21) retrieved 27 November 2021 from https://techxplore.com/news/2020-02-coding-uncertainty.html