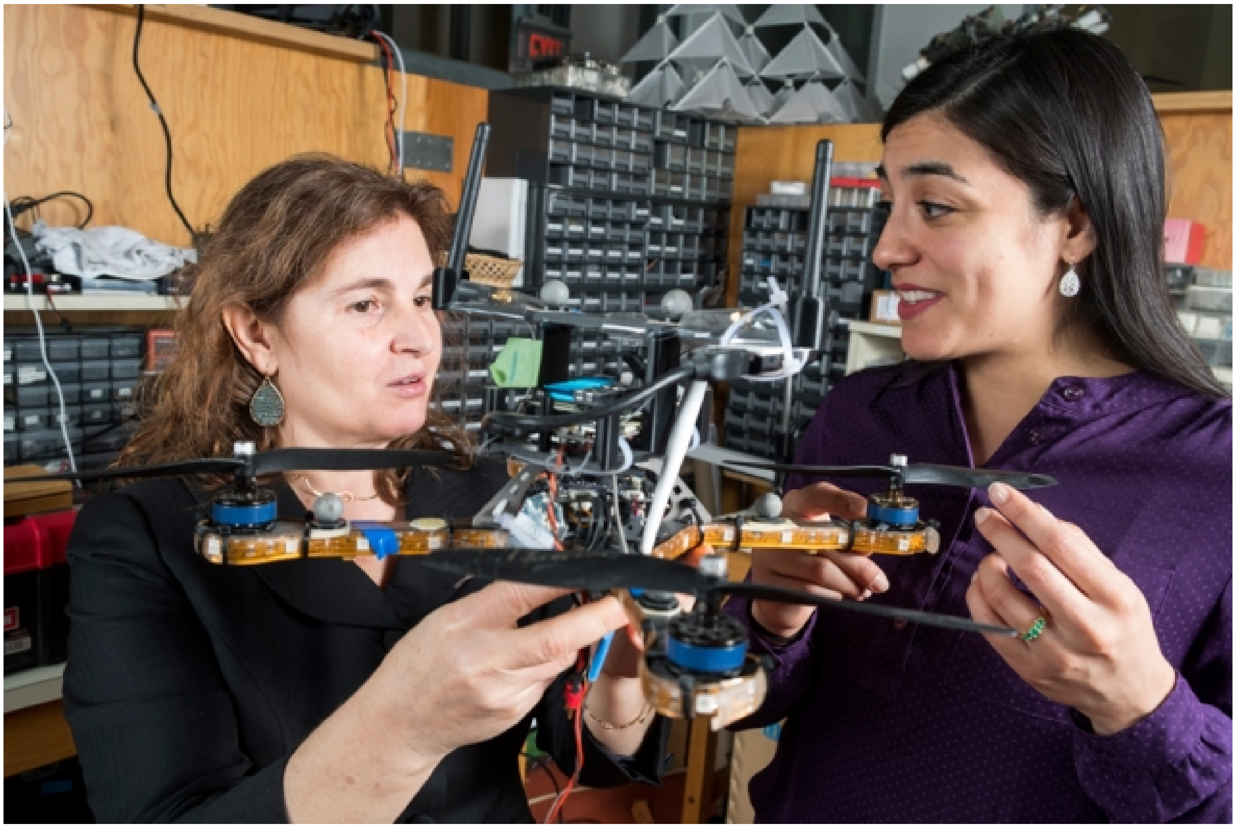
Technique could protect robot teams' communication networks from malicious hackers

March 17 2017, by Larry Hardesty



Researchers including MIT professor Daniela Rus (left) and research scientist Stephanie Gil (right) have developed a technique for preventing malicious hackers from commandeering robot teams’ communication networks. To verify the theoretical predictions, the researchers implemented their system using a battery of distributed Wi-Fi transmitters and an autonomous helicopter. Credit: M. Scott Brauer

Distributed planning, communication, and control algorithms for autonomous robots make up a major area of research in computer science. But in the literature on multirobot systems, security has gotten relatively short shrift.

In the latest issue of the journal *Autonomous Robots*, researchers from MIT's Computer Science and Artificial Intelligence Laboratory and their colleagues present a new technique for preventing malicious hackers from commandeering robot teams' communication networks. The technique could provide an added layer of security in systems that encrypt communications, or an alternative in circumstances in which encryption is impractical.

"The robotics community has focused on making multirobot systems autonomous and increasingly more capable by developing the science of autonomy. In some sense we have not done enough about systems-level issues like cybersecurity and privacy," says Daniela Rus, an Andrew and Erna Viterbi Professor of Electrical Engineering and Computer Science at MIT and senior author on the new paper.

"But when we deploy multirobot systems in real applications, we expose them to all the issues that current computer systems are exposed to," she adds. "If you take over a computer system, you can make it release private data—and you can do a lot of other bad things. A cybersecurity attack on a robot has all the perils of attacks on computer systems, plus the robot could be controlled to take potentially damaging action in the physical world. So in some sense there is even more urgency that we think about this problem."

Identity theft

Most planning algorithms in multirobot systems rely on some kind of voting procedure to determine a course of action. Each robot makes a recommendation based on its own limited, local observations, and the recommendations are aggregated to yield a final decision.

A natural way for a hacker to infiltrate a multirobot system would be to impersonate a large number of robots on the network and cast enough spurious votes to tip the collective decision, a technique called "spoofing." The researchers' new system analyzes the distinctive ways in which robots' wireless transmissions interact with the environment, to assign each of them its own radio "fingerprint." If the system identifies multiple votes as coming from the same transmitter, it can discount them as probably fraudulent.

"There are two ways to think of it," says Stephanie Gil, a research scientist in Rus' Distributed Robotics Lab and a co-author on the new paper. "In some cases cryptography is too difficult to implement in a decentralized form. Perhaps you just don't have that central key authority that you can secure, and you have agents continually entering or exiting the network, so that a key-passing scheme becomes much more challenging to implement. In that case, we can still provide protection.

"And in case you can implement a cryptographic scheme, then if one of the agents with the key gets compromised, we can still provide protection by mitigating and even quantifying the maximum amount of damage that can be done by the adversary."

“A cybersecurity attack on a robot has all the perils of attacks on computer systems, plus the robot could be controlled to take potentially damaging action in the physical world. So in some sense there is even more urgency that we think about this problem,” says Rus. Credit: M. Scott Brauer

Hold your ground

In their paper, the researchers consider a problem known as "coverage," in which robots position themselves to distribute some service across a geographic area—communication links, monitoring, or the like. In this case, each robot's "vote" is simply its report of its position, which the other robots use to determine their own.

The paper includes a theoretical analysis that compares the results of a common coverage algorithm under normal circumstances and the results produced when the new system is actively thwarting a spoofing attack. Even when 75 percent of the robots in the system have been infiltrated by such an attack, the robots' positions are within 3 centimeters of what they should be. To verify the theoretical predictions, the researchers also implemented their system using a battery of distributed Wi-Fi transmitters and an autonomous helicopter.

"This generalizes naturally to other types of algorithms beyond coverage," Rus says.

The new system grew out of an earlier project involving Rus, Gil, Dina Katabi—who is the other Andrew and Erna Viterbi Professor of Electrical Engineering and Computer Science at MIT—and Swarun Kumar, who earned master's and doctoral degrees at MIT before moving to Carnegie Mellon University. That project sought to use Wi-Fi signals to determine transmitters' locations and to repair ad hoc communication networks. On the new paper, the same quartet of researchers is joined by MIT Lincoln Laboratory's Mark Mazumder.

Typically, radio-based location determination requires an array of receiving antennas. A radio signal traveling through the air reaches each of the antennas at a slightly different time, a difference that shows up in the phase of the received signals, or the alignment of the crests and troughs of their electromagnetic waves. From this phase information, it's possible to determine the direction from which the signal arrived.

Space vs. time

A bank of antennas, however, is too bulky for an autonomous helicopter to ferry around. The MIT researchers found a way to make accurate location measurements using only two antennas, spaced about 8 inches apart. Those antennas must move through space in order to simulate measurements from multiple antennas. That's a requirement that autonomous robots meet easily. In the experiments reported in the new paper, for instance, the autonomous helicopter hovered in place and rotated around its axis in order to make its measurements.

When a Wi-Fi transmitter broadcasts a signal, some of it travels in a direct path toward the receiver, but much of it bounces off of obstacles in the environment, arriving at the receiver from different directions. For location determination, that's a problem, but for radio fingerprinting, it's an advantage: The different energies of signals arriving from different directions give each transmitter a distinctive profile.

There's still some room for error in the receiver's measurements, however, so the researchers' new system doesn't completely ignore probably fraudulent transmissions. Instead, it discounts them in proportion to its certainty that they have the same source. The new paper's theoretical analysis shows that, for a range of reasonable assumptions about measurement ambiguities, the system will thwart spoofing attacks without unduly punishing valid transmissions that happen to have similar fingerprints.

"The work has important implications, as many systems of this type are on the horizon—networked autonomous driving cars, Amazon delivery drones, et cetera," says David Hsu, a professor of computer science at the National University of Singapore. "Security would be a major issue for such systems, even more so than today's networked computers. This solution is creative and departs completely from traditional defense mechanisms."

More information: Stephanie Gil et al. Guaranteeing spoof-resilient multi-robot networks, *Autonomous Robots* (2017). DOI: 10.1007/s10514-017-9621-5

This story is republished courtesy of MIT News (web.mit.edu/newsoffice/), a popular site that covers news about MIT research, innovation and teaching.

Provided by Massachusetts Institute of Technology

Citation: Technique could protect robot teams' communication networks from malicious hackers (2017, March 17) retrieved 9 April 2024 from https://techxplore.com/news/2017-03-technique-robot-teams-networks-malicious.html