To keep drones out of high-risk areas, companies try hijacking them and shooting them down

October 26 2016, by Samantha Masunaga, Los Angeles Times

A public awareness campaign last year did little to deter the growing number of rogue drones flying near wildfires and forcing firefighters to ground their own aircraft.

So this year, the Department of the Interior tried something a little more direct.

The agency gave real-time access to data on all active wildfires to two airspace mapping companies as part of a pilot program.

One of those firms, AirMap, worked with drone manufacturer DJI, which created "geofences" around wildfires. When drones hit the virtual boundary, the geofencing software overrides the flight controller and forces them to hover in place. Any drone deployed inside the barrier won't be able to lift off.

"We really want to have this new community of pilots be as responsible as the manned aircraft pilots that came before them," said Mark Bathrick, director of the office of aviation services at the Department of the Interior.

As private drone use has soared, so has concern about keeping the remote-controlled aircraft away from sensitive and high-risk areas such as airports, nuclear power plants and prisons.

Those concerns are heightened by high-profile incidents such as the near collision in March of a drone and a Lufthansa jet approaching Los Angeles International Airport. In 2013 a drone crash landed in front of German Chancellor Angela Merkel at a campaign event, and a quadcopter crashed on the White House lawn in 2015.

Defense giants Boeing Co. and Lockheed Martin Corp., as well as a handful of startups, have jumped into the fray, developing technology ranging from detection systems to more disruptive solutions such as software that forces unauthorized drones to go home or land safely and laser cannons that shoot unwanted drones out of the sky.

The technology is of interest to commercial users as well as the government. The Department of Defense hosts an annual counterdrone demonstration called Black Dart in which the military, its allies and industry partners can assess current technology and techniques.

Earlier this year, the Federal Aviation Administration tested FBI drone-detection technology at John F. Kennedy International Airport in New York and Atlantic City International Airport in New Jersey for a few weeks.

Last year, Boeing unveiled its compact laser weapons system, which ignites targeted drones. At a demonstration in California, Boeing said it took only about 15 seconds for its 2-kilowatt laser to disable the drone.

Though the counterdrone industry is still nascent, the global market - including both civilian and military uses - could be worth at least several hundreds of millions of dollars, said Michael Blades, senior industry analyst for aerospace and defense at research and consulting firm Frost & Sullivan.

"With all the talk of how many drones are going to be flying around and, at least on the commercial side, how much privacy is going to be an issue, I think these companies saw an opportunity," he said.

Much will depend on how well the technology works. It's not easy to devise a system that tracks and identifies tiny drones, and stops unauthorized ones without knocking out everything - or creating a safety hazard.

"This rapid proliferation of startups, of large companies all proposing systems that deal with the issue in different ways, suggests to me that there isn't one single unifying solution for how to bring drones out of the sky," said Arthur Holland Michel, co-director of the Center for the Study of the Drone at Bard College in New York. "Every single step of the process is challenging."

That starts with identifying whether drones are friendly or rogue.

Autonomous drone-detection systems need to be sophisticated enough to distinguish between slow-moving drones and birds, or even the signals emitted from drones compared with those emitted by cellphones.

Detection systems will likely need to integrate a number of sensors such as acoustics, cameras, radio frequency or even radar to create "multilayer capability," Blades said.

Other companies and organizations are looking into the interdiction, or disruptive, aspect of how to safely deal with a drone threat once it is identified.

At Aerospace Corp., researchers are investigating how to isolate the link between a specific drone and its controller that could lead to a safe takeover - rather than blindly "jamming," or interrupting, all of the authorized frequencies in that range to cause confusion and force a potentially unpredictable landing. It is illegal for nongovernment entities to operate these kinds of jammers.

That sounds easier than it is. Drones change their frequency band tens of times a second to ensure an uninterrupted communications link, said Randy Villahermosa, principal director of research and program development at Aerospace Corp. But by using software-defined radios and integrating the team's coding knowledge, the researchers have been able to successfully take over a drone's controls in several tests, said Esteban Valles, associate director of digital communication in the implementation department at Aerospace Corp.

The researchers have also worked on pinpointing the position of a rogue drone's controller, allowing law enforcement to find the pilot.

There have been more than 300 so-called drone incidents in California between April 2014 and Jan. 31, 2016, according to an analysis of FAA data by U.S. Sen. Dianne Feinstein's office. More than half of these incidents involved a drone that flew within 5 miles of an airport.

In one case from early January, a Cessna agricultural aircraft reported that it possibly hit a drone about 1,400 feet in the air near Modesto, according to the analysis. No damage was reported to the aircraft.

Aerospace Corp. does not sell its products commercially but is trying to better understand how drone communications work so it can advise customers on their own technology solutions, Villahermosa said.

Drone maker DJI introduced its GPS-based geofence system about three years ago. It prevents "inadvertent" drone operations in sensitive areas, such as airports or in Washington, D.C.

Since drones rely on their GPS receivers to determine where they are, DJI preprograms certain locations into the geofencing system. If a drone gets close to one of these locations, operators first receive a warning, said Brendan Schulman, vice president of policy and legal affairs at DJI. If they continue to fly their drone, they will be stopped by the geofence. The distance around these sensitive locations can vary.

A more recent version includes locations with a temporary flight restriction, such as sporting events.

DJI, which analysts estimate sells up to 70 percent of all consumer and professional drones, has included the option of overriding the geofence for wildfires, allowing a "verified" user to input credit card information or a mobile phone number to give firefighting or other authorized personnel the ability to keep using drones for legitimate efforts.

"It's really a balance between safety and innovation," Schulman said. "We don't want to just shut down the technology in places it can be useful."

Citation: To keep drones out of high-risk areas, companies try hijacking them and shooting them down (2016, October 26) retrieved 25 April 2024 from https://phys.org/news/2016-10-drones-high-risk-areas-companies-hijacking.html