Real-time drone intent monitoring could enable safer use of drones and prevent a repeat of 2018 Gatwick incident

September 15 2021

Credit: CC0 Public Domain

Researchers have developed a real-time approach that can help prevent incidents like the large-scale disruption at London's Gatwick Airport in

2018, where possible drone sightings at the perimeter of the airport caused the cancellation of hundreds of flights.

The researchers, from the University of Cambridge, used a combination of statistical techniques and radar data to predict the flight path of a drone, and whether it intends to enter a restricted airspace, for instance around a civilian airport.

Their solution could help prevent a repeat of the Gatwick incident, as it can spot any drones before they enter restricted airspace and can determine, early, if their future actions are likely to pose a threat to other aircraft.

This new predictive capability can enable automated decision making and significantly reduce the workload on drone surveillance system operators by offering actionable information on potential threats to facilitate timely and proportionate responses.

Real radar data from live drone trials at several locations was used to validate the new approach. Some of the results will be reported today (15 September) at the Sensor Signal Processing for Defence Conference in Edinburgh.

Drones have become ubiquitous over the past several years, with widespread applications in agriculture, surveying and e-commerce, among other fields. However, they can also be a nuisance or present a potential safety risk, especially with the wide availability of cheap and increasingly more capable platforms.

A few days before Christmas 2018, reported drone sightings near the perimeter of Gatwick Airport caused hundreds of flights to be disrupted due to the possible risk of collision. No culprit was found.

"While we don't fully know what happened at Gatwick, the incident highlighted the potential risk drones can pose to the public if they are misused, whether that's done maliciously or completely innocently," said paper co-author Dr. Bashar Ahmad, who carried out the research while based at Cambridge's Department of Engineering. "It's crucial for future drone surveillance systems to have predictive capabilities for revealing, as early as possible, a drone with malicious intent or anomalous behaviour."

To aid with air traffic control and prevent any possible collisions, commercial airplanes report their location every few minutes. However, there is no such requirement for drones.

"There needs to be some sort of automated equivalent to air traffic control for drones," said Professor Simon Godsill from Cambridge's Department of Engineering, who led the project. "But unlike large and fast-moving targets, like a passenger jet, drones are small, agile, and slow-moving, which makes them difficult to track. They can also easily be mistaken for birds, and vice versa."

"We need to spot threats as early as possible, but we also need to be careful not to overreact, since closing civilian airspace is a drastic and highly disruptive measure that we want to avoid, especially if it ends up being a false alarm," said first author Dr. Jiaming Liang, also from the Department of Engineering, who developed the underlying algorithms with Godsill.

There are several potential ways to monitor the space around a civilian airport. A typical drone surveillance solution can use a combination of several sensors, such as radar, radio frequency detectors and cameras, but it's often expensive and labour-intensive to operate.

Using Bayesian statistical techniques, the Cambridge researchers built a

solution that would only flag those drones which pose a threat and offer a way to prioritise them. Threat is defined as a drone that's intending to enter restricted airspace or displays an unusual flying pattern.

"We need to know this before it happens, not after it happens," said Godsill. "This way, if a drone is getting too close, it could be possible to warn the drone operator. For obvious safety reasons, it's prohibited to disable a drone in civilian airspace, so the only option is to close the airspace. Our goal is to make sure airport authorities don't have to do this unless the threat is a real one."

The software-based solution uses a stochastic, or random, model to determine the underlying intent of the drone, which can change dynamically over time. Most drones navigate using waypoints, meaning they travel from one point to the next, and a single journey is made of multiple points.

In tests using real radar data, the Cambridge-developed solution was able to identify drones before they reached their next waypoint. Based on a drone's velocity, trajectory and other data, it was able to predict the probability of any given drone reaching the next waypoint in real time.

"In tests, our system was able to spot potential threats in seconds, but in a real scenario, those seconds or minutes can make the difference between an incident happening or not," said Liang. "It could give time to warn incoming flights about the threat so that no one gets hurt."

The Cambridge researchers say their solution can be incorporated into existing surveillance systems, making it a cost-effective way of tracking the risk of drones ending up where they shouldn't. The algorithms could, in principle, also be applied to other domains such as maritime safety, robotics and self-driving cars.