Research highlights need to safeguard drones and robotic cars against cyber attacks

November 27 2019

Credit: CC0 Public Domain

Robotic vehicles like Amazon delivery drones or Mars rovers can be hacked more easily than people may think, new research from the University of British Columbia suggests.

The researchers, based at UBC's faculty of applied science, designed

three types of stealth attack on robotic vehicles that caused the machines to crash, miss their targets or complete their missions much later than scheduled.

The attacks required little to no human intervention to succeed on both real and simulated drones and rovers.

"We saw major weaknesses in robotic vehicle software that could allow attackers to easily disrupt the behaviour of many different kinds of these machines," said Karthik Pattabiraman, the electrical and computer engineering professor who supervised the study. "Especially worrisome is the fact that none of these attacks could be detected by the most commonly used detection techniques."

Robotic vehicles use special algorithms to stay on track while in motion, as well as to flag unusual behaviour that could signal an attack. But some degree of deviation from the travel plan is typically allowed to account for external factors like friction and wind—and it's these deviations that attackers can exploit to throw the vehicles off course.

The UBC team developed an automated process that enables an attacker to quickly learn the allowed deviations of robotic vehicles running conventional protection systems. Hackers can then use the information to launch a series of automated attacks that the vehicle cannot detect until it's too late.

"Robotic vehicles are already playing an important role in surveillance, warehouse management and other contexts, and their use will only become more widespread in the future," says Pritam Dash, an electrical and computer engineering graduate student at UBC and the study's lead author. "We need safety measures to prevent rogue drones and rovers from causing serious economic, property and even bodily harm."

The researchers offer the basis for a few such countermeasures—including self-adjusting deviation thresholds—in a recent paper describing their findings. They will present their work at the Annual Computer Security Applications Conference in San Juan, Puerto Rico, next month.

More information: Pritam Dash et al, Out of control, *Proceedings of the 35th Annual Computer Security Applications Conference on - ACSAC '19* (2019). DOI: 10.1145/3359789.3359847

Provided by University of British Columbia