Game of Drones: Detecting Streamed POI from Encrypted FPV Channel

Researchers

Ben Nassi
nassidt@gmail.com

Raz Ben-Netanel
razx@post.bgu.ac.il

Prof. Adi Shamir
adi.shamir@weizmann.ac.il

Prof. Yuval Elovici
elovici@inter.net.il

Publication

B. Nassi, R. Ben-Netanel, A. Shamir, and Yuval Elovici, "Game of Drones - Detecting Streamed POI from Encrypted FPV Channel, 2018. arXiv:1801.03074.

Goals

Drones have created a new threat to people's privacy. We are now in an era in which anyone with a drone equipped with a video camera can use it to invade a subject's privacy by streaming the subject in his/her private space over an encrypted first person view (FPV) channel. Although many methods have been suggested to detect nearby drones, they all suffer from the same shortcoming: they cannot identify exactly what is being captured, and therefore they fail to distinguish between the legitimate use of a drone (for example, to use a drone to film a selfie from the air) and illegitimate use that invades someone's privacy (when the same operator uses the drone to stream the view into the window of his neighbor's apartment), a distinction that in some cases depends on the orientation of the drone's video camera rather than on the drone's location.

Description

We challenge the commonly held belief that the use of encryption to secure an FPV channel prevents an interceptor from extracting the POI that is being streamed. We show methods that leverage physical stimuli to detect whether the drone's camera is directed towards a target in real time. We investigate the influence of changing pixels on the FPV channel (in a lab setup). Based on our observations we demonstrate how an interceptor can perform a side-channel attack to detect whether a target is being streamed by analyzing the encrypted FPV channel that is transmitted from a real drone (DJI Mavic) in two use cases: when the target is a private house and when the target is a subject.