Demo: Identifying Drones Based on Visual Tokens

Ben Nassi[1], Elad Feldman[1], Aviel Levy[1], Yaron Pirutin[1], Asaf Shabtai[1], Ryusuke Masuoka[2], Yuval Elovici[1]
[1]Ben-Gurion University of the Negev, [2]Fujitsu System Integration Laboratories
{nassib,eladfeld, aviellev, yaronpir, shabtaia, elovici}@post.bgu.ac.il, masuoka.ryusuke@fujitsu.com
Video Demonstration: https://drive.google.com/file/d/1V1Y_n6kN7FpICqkRrGRGhukk2Cfprrpy/view

Motivation. The use of drones is rapidly increasing in many parts of the world, where drones are now used for a number of vital applications (e.g., disaster relief, rescue missions, and fire detection). This fact can be exploited by attackers in order to infiltrate a similar looking foe drone that can perform malicious activities (e.g., spying, terrorism, smuggling), which, owing to the drones' similar appearance, would not arouse suspicion. As a result, there is a need for a method that third parties can use to authenticate similar looking foe and friend drones and differentiate between them (see Figure 1).

Scientific Gap. Current authentication methods authenticate a drone based on radio-frequency (RF) protocols. Such protocols, which usually consist of information required to detect the drone (e.g., ID, GPS coordinates), are used to physically authenticate the drone (e.g., by a video camera) based on the digital radio transmission. However, given the known average GPS error under open skies (4.9 meters), a question arises: how can we distinguish between two drones when one (a foe drone used to perform an illegitimate activity) infiltrates the aerial area of another (a similar looking friend drone performing a legitimate activity) when they are less than 4.9 meters apart?

This demo shows how we overcome this vulnerability using a new method for distinguishing between two identical looking drones.

Suggested Method. In this method, drones are identified by a video camera based on messages visually broadcast from a device carried by the drone which consists of an LED strip (see Figure 2). The messages can take the form of visual RSA tokens that are used to authenticate the drone over time. A machine learning model is used to convert the visual signals to a binary message, and the drone is identified by comparing the message obtained from the visual stream to the message obtained from the RF signal.

Experiment. The experiment was conducted under various conditions: at different times of the day and night, using various backgrounds, and varying the distance between the drone and the camera (50, 100, 150, and 200 meters). The

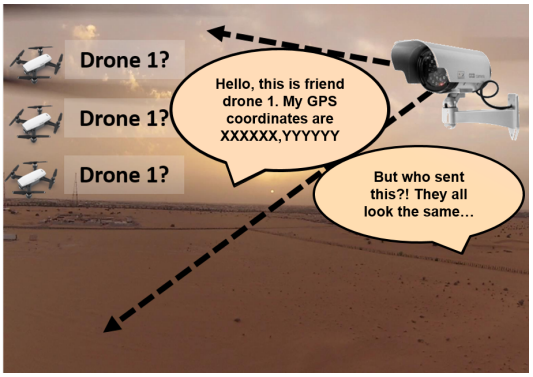

Fig. 1. The remote drone identification challenge: distinguishing between several similar looking drones located in close proximity to one another.

Fig. 2. The authenticatee device mounted on a drone to transmit message.

flashes from the LED and LCD were intercepted by the camera and decoded by a machine learning model to a message. Two different types of authentication devices – a flashing light and an LCD screen – were used to transmit the message; we also attempted to send the message using both devices in combination.

Results We achieved 90% precision, on average, in decoding the content of the messages used to authenticate the drone. This results can be further improve using error correction code.

An extended version of this paper, which includes the algorithm used to receive the message and distinguish between the drones, is available [1].

References

[1] B. Nassi, A. Levy, Y. Pirutin, A. Shabtai, R. Masuoka, and Y. Elovici, "Redroid: Remote drone identification based on visual rsa securid tokens," in *2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*, 2021, pp. 1–9.

Workshop on Automotive and Autonomous Vehicle Security (AutoSec) 2022
24 April 2022, San Diego, CA, USA
ISBN 1-891562-75-4
https://dx.doi.org/10.14722/autosec.2022.23002
www.ndss-symposium.org