USING RADIO FREQUENCY SIGNAL FINGERPRINTS FOR DRONE DETECTION

Dimitrie C. Popescu | *Department of Electrical and Computer Engineering, Old Dominion University*

INTRODUCTION

Unmanned autonomous vehicles (UAVs or drones) have become very affordable in recent years and they are currently used in a wide range of applications that include surveillance, search and rescue missions, infrastructure inspections, or package delivery to name just a few.

We note that unrestricted drone operation has the potential to endanger public safety, and that reports of drones used for malicious activities such as cyberattacks or espionage have been reported [1]. Thus, accurate detection and classification of drones and of their activity is important for both public safety and national security.

UAV DETECTION SYSTEM

- A promising technique for passive drone detection is based on eavesdropping on the radio communication between drones and their controllers, shown in Fig. 1.

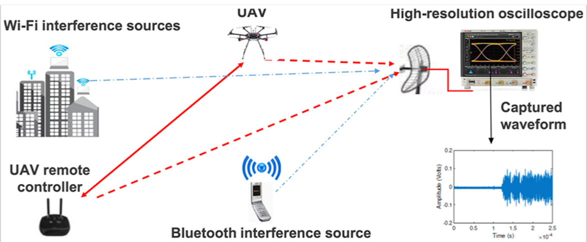

Fig. 1. RF-based drone detection in the presence of interference [2]

- RF signals transmitted to control the drones are recorded and analyzed in order to determine specific features, referred to as RF fingerprints.
- The RF fingerprints depend on the physical and MAC layer characteristics of the radio link between the drone and its controller.

RF-BASED DRONE DETECTION

- Once an active RF signal is detected, MAC layer features of the signal can be used for drone detection and classification.
- Most commercially available drones operate in un-licensed frequency bands that are also used by Wi-Fi and mobile Bluetooth devices, which act as interfering sources for the drone detection system [2].
- RF-based drone detection systems consist of two main stages:
  - 1st stage: active RF-signals intended for a drone are distinguished from interfering signal
  - 2nd stage: the captured signal is processed to extract specific features from its energy-time-frequency domain representation

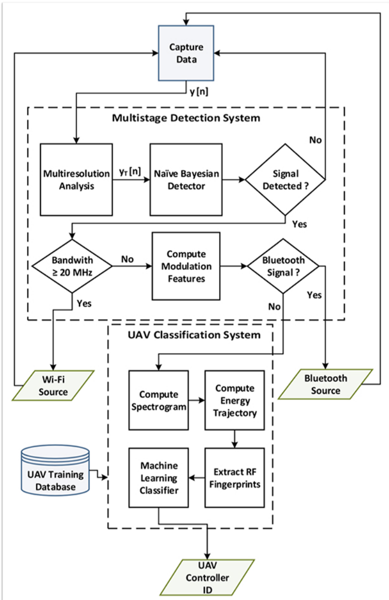

Fig. 2. System flowchart for detection and classification of RF signals in presence of interference [2]

RESULTS AND CONCLUSIONS

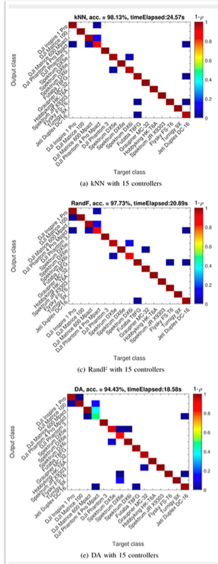

Fig. 3. Confusion matrices of kNN, RandF, and DA classifiers based on 3 RF fingerprints [2]

The system was successful in detecting and classifying UAV signals in the presence of interference.

For 15 controllers, the accuracy of the following classifiers, as shown in Fig. 3 are:

- kNN = 98.13%
- RandF = 97.73%
- DA = 94.43% [2]

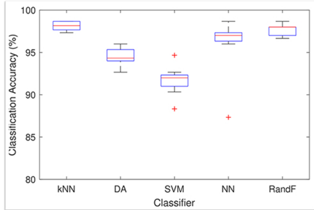

Fig. 4. Box plot of the classification accuracy for 15 controllers based on 3 RF fingerprints[2]

REFERENCES

[1] H. Shakhatreh *et al.*, "Unmanned Aerial Vehicles (UAVs): A Survey on Civil Applications and Key Research Challenges," in *IEEE Access*, vol. 7, pp. 48572-48634, 2019 (doi: 10.1109/ACCESS.2019.2909530).

[2] M. Ezuma, F. Erden, C. K. Anjinappa, O. Ozdemir and I. Guvenc, "Detection and Classification of UAVs Using RF Fingerprints in the Presence of Wi-Fi and Bluetooth Interference," in *IEEE Open Journal of the Communications Society, 2019* (doi: 10.1109/OJCOMS.2019.2955889).

ACKNOWLEDGEMENTS

Abigail Stedman, MS student, ECE Department, Old Dominion University