Drone detection and neutralisation system using electronic warfare technologies

Author: mgr inż. Przemysław Flak

ABSTRACT

The history of the development of unmanned aerial vehicles, also known as drones, shows that, despite their initial military-oriented design, technological advances have contributed to a significant increase in their civilian deployment. The introduction of drones for commercial applications has opened up entirely new opportunities for many sectors of the industry, due to the exceptional versatility of these devices. Unfortunately, the growing demand for aerial services, the high availability of amateur solutions, and the low barrier of entry into the world of unmanned aerial vehicles have also unleashed a new category of threats, not only to critical infrastructure but also to everyday life.

The aim of this dissertation is to review methods and provide a solution for detecting and counteracting malicious activities resulting from the use of commercial unmanned aerial vehicles. The radio-electronic approach, based on the ability to identify and classify sources of electromagnetic emissions and, consequently, to disrupt their operation, has been selected for further analysis. Although the range of counter-drone systems in this category is often defined as several kilometres, field conditions, propagation effects, and urban development significantly limit its effectiveness. In addition, the cost of these solutions, combined with the need for high computing power, makes it difficult to scale this approach in applications where large areas need to be protected.

The featured research work covers not only the evaluation of known techniques and algorithms but also the development of a proprietary solution tailored to a specific operational scenario. An important aspect of the project is also the creation of a physical prototype of a device based on off-the-shelf components and the characterisation of its capabilities in relation to specific operational conditions. The concept of a distributed network of detectors and effectors with local processing, limiting the need for very high data link throughput, has been tested in simulated and near-real conditions.

Based on a commercial electronic circuit, the author made changes to the software to increase the contribution of the hardware layer in the processes of detecting radio signals based on time-frequency recordings. Algorithms for identifying transmissions from unmanned aerial vehicles using machine learning techniques were also proposed, which were analysed with reference to either an open or proprietary signature database. The last part of the work presents experiments confirming the effector's ability to jam satellite navigation signals and those used for remote control of drone systems. The result of this thesis is a prototype that can serve both as a standalone indicator of the presence of unwanted objects in the vicinity and as an essential element for the implementation of the distributed architecture concept.