2020/2500M-0117

ISSN 1797-3457 (verkkojulkaisu)
ISBN (PDF) 978-951-25-3341-1

SUMMARY REPORT

ELECTRONIC INTERCEPTION OF UNMANNED AERIAL VEHICLES (MIEHITTÄMÄTTÖMIEN ILMA-ALUSTEN ELEKTRONINEN TORJUNTA)

Taneli Riihonen (email: taneli.riihonen@tuni.fi; phone: +358-50-447 8349), Mikko Heino, Jaakko Marin, Karel Pärlin, Matias Turunen, and Miika Vuorenmaa

Unit of Electrical Engineering, Tampere University, Finland

Abstract: One of the fastest evolving threats within the security and defense sector is drones and, thus, counter-drone capabilities are becoming more and more important. Amongst the principal methods for countering drones and swarms thereof is to target the radio signals from aerial vehicles and their ground control stations. Ideally, drone reconnaissance and neutralization would happen simultaneously. However, carrying out transmit-and-receive electronic warfare operations in the same frequency band simultaneously is impossible with conventional radio technology, thus spectrum division methods with various performance penalties are employed conventionally. We studied how to enhance defense capabilities against drone swarms by developing novel, disruptive counter-drone competencies based on full-duplex (FD) radio technology and machine learning (ML), resulting in enhanced situational awareness, improved neutralization performance, multifunction capabilities, and minimized collateral damage.

1. Introduction

The number of drones sold globally has rapidly increased over the past decade and it is estimated that this proliferation will certainly continue over the coming years. Small drones are quite simple systems and their concepts do not differ considerably for commercially available drones and military surveillance assets. Still, both can be used by an adversary. Technically such systems consist of an aerial vehicle (or several in the case of swarming), a ground control station, and wireless data links connecting them. Given the wide range of possible uses for drones, it is not surprising that the number of reports of malicious use within the civilian domain are on the rise (e.g., airport interruptions, drug deliveries, illegal surveillance, and kinetic attacks). The level of threat posed by drones is also growing within the defense sector as drones are becoming a recognized tool in hybrid warfare context; they pose a threat, e.g., in the form of gathering intelligence and attacking through the delivery of explosives. It is anticipated that, driven by the civilian market, drone technology will continue to progress quickly and the capabilities of drones in terms of speed, flight time, payload capacity, autonomy, low detectability, and swarm functionality will improve. Those features consequently increase the threat level posed by drone swarms to both the armed forces and civilian/commercial security.

Counter-drone solutions are being developed globally to mitigate the growing threat. The countermeasures are typically considered in four stages from detecting to neutralizing through locating and identifying (see Fig. 1). Because individual drones and drone swarms very often rely on radio frequency (RF) communications for the control and coordination of operations, RF-based methods for detecting and neutralizing drones are prominent. Besides the electromagnetic spectrum, drones increasingly make use of also non-RF-based sensors and sensor fusion. Therefore, despite this research project focused on the RF-based counter-drone methods, one should bear in mind that they need to be accompanied also by other methods for achieving robust counter-drone capabilities.

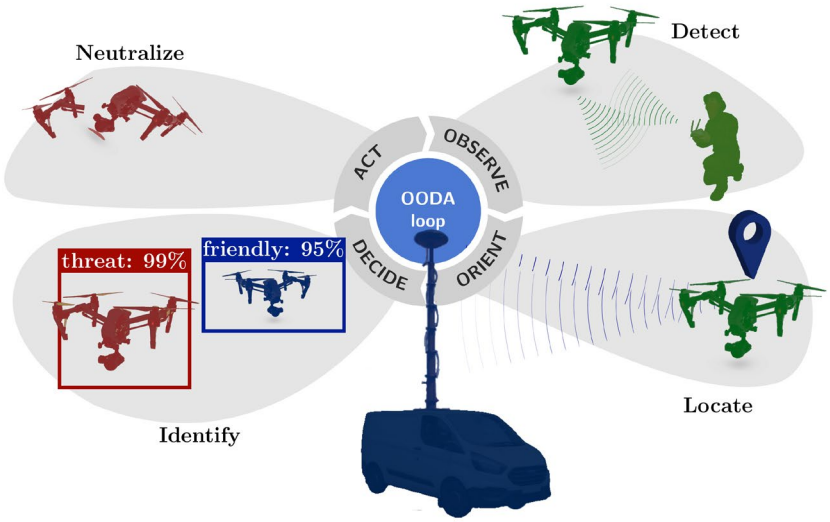


Figure 1. The typical four stages of countering drones [10].

2. Research objectives and accomplishment plan

The general objective of the research project was to develop smart radio technology for detecting and neutralizing drones and drone swarms. Before the actual scientific research, we pursued groundwork for establishing this new research area in Finland. The original research work considered the application of the so-called full-duplex (FD) radio technology and machine learning (ML) for advanced counter-drone systems.

2.1. Groundwork for the research

Before we could pursue original research on counter-drone technologies, we needed to investigate what kind of radio signals are employed by drone systems in the market. In other words, we needed to know what to detect and what to jam. These were not trivial questions since there are no standardized protocols, but every manufacturer has their own and even different models from a vendor may be incompatible. We planned to find the answers by reverse engineering a comprehensive set of drones' radio signals.

The second direction for groundwork was to develop a laboratory testbed for experiments on detection and jamming of drone radio-control (RC) systems. The testbed is important for the research line in two ways: It allows for achieving reproducible results in a controlled environment and overcomes the need for open-air experiments using actually flying drones, which obviously render many practical problems in implementation.

2.2. Full-duplex radio technology

Modern radio technology, including both drone and counter-drone radio techniques, has evolved into its current state with the assumption that same-frequency simultaneous transmit-and-receive operation is impossible. However, recent research is forcing a paradigm shift as this assumption is being overturned in the form of full-duplex operation — perhaps igniting an arms race between drone and counter-drone technology for this superpower. The full-duplex radio technology originates from the communication context, from which we transferred it to the electronic warfare context. The objective of the research was to apply and develop new full-duplex radio technology for simultaneously detecting and jamming drones as well as to demonstrate the feasibility of the concept.

2.3. Machine learning for counter-drone systems

To effectively counter malicious drones, the defense systems need to be able to detect a new drone entering a restricted airspace, locate its position, identify its purpose, and

(should the identification procedure mark it as a threat) neutralize it. The operations within these stages are illustrated in Fig. 1. Each of them can be realized through various sensors and methods, which conventionally have been controlled by handcrafted algorithms. However, continuous advances in machine learning could be the key for an endless improvement of counter-drone systems' techniques and abilities, providing them with an advantage that could eventually make them invincible in the field.

Especially neural networks (NNs) are increasingly considered as key constituents of drone security systems in recent research efforts. In fact, a substantial number of surveillance systems relying on NNs have been successfully implemented and commercialized. In addition to analyzing data from any given sensor, machine learning might prove crucial in aggregating data obtained from multiple sensors of different types through sensor fusion, which leads to enhanced situational awareness. In this research project, we studied how NNs are used to enhance the four stages of drone threat mitigation, collected references to bibliographic surveys devoted to counter-drone security systems featuring NNs, and drew attention to potential research opportunities we envision in this field.

3. Materials and methods

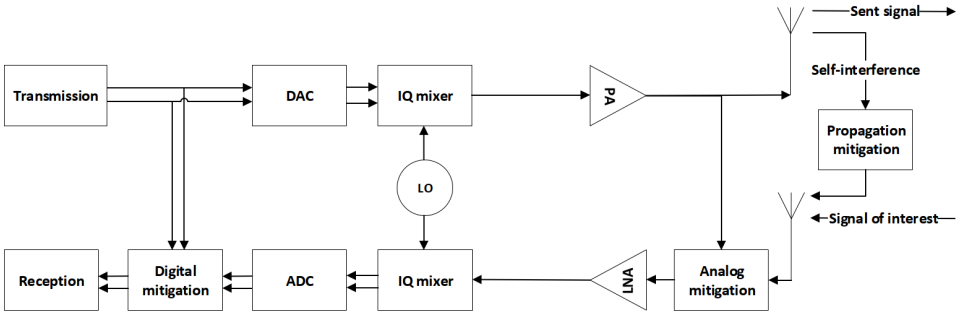
Firstly, the project utilized existing scientific knowledge available in the open literature as the primary research material. Full-duplex radios are a well-established, emerging technology for communications purposes, where typically the direct-conversion architecture illustrated in Fig. 2(a) is applied, or the cancellation signal can be generated also by a separate transmit chain [2]. An alternative transceiver architecture, which is illustrated in Fig. 2(b), is conventionally used in frequency-modulated continuous-wave (FMCW) radars so that this area offers good material for transferring the concept into the original full-duplex applications. Likewise, machine learning has advanced tremendously during the last few years. Especially, we studied many bibliographic surveys devoted to counter-drone security systems featuring neural networks (cf. references in [10]).

Secondly, we utilized radio devices for the experimental results. Several consumer drones were borrowed as research material for the project. In particular, we studied the uplink control and downlink video signals of the following ten popular drone models: DJI Inspire 2, DJI Matrice 100, DJI Matrice 210, DJI Mavic Mini, DJI Mavic Pro, DJI Phantom 4, DJI Phantom 4 Pro+, Parrot Disco, Parrot Mambo, and Yuneec Typhoon H. We even had got two different devices of some models for comparing different versions. Furthermore, we utilized laboratory equipment such as an oscilloscope, a vector-signal transceiver, and a spectrum analyzer for constructing the testbed and conducting the experiments.

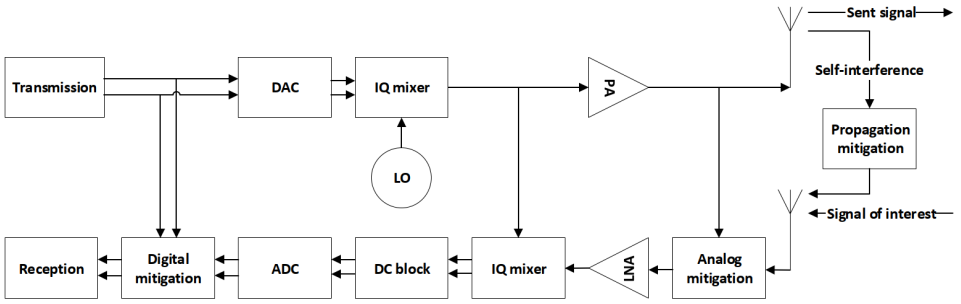
As indicated by the above, the primary research methods were theoretical investigations by surveying open literature and practical experiments in a laboratory. Furthermore, the radar-inspired transceiver architecture was analyzed based on computer simulations too.

4. Results and discussion

The groundwork laid solid foundations for the research line as planned. Especially creating the dataset of drones' radio signals represents a significant advance and is valuable to the scientific community at large. The main outcomes from the original research were the characterization of the radar-inspired transceiver architecture for full-duplex multifunction radios as well as the experimental and theoretical studies of neural networks for counter-drone systems. The results were reported in the scientific publications [1] through [10]. In addition to the technical outcomes, the project contributed to international collaboration within the research task group (RTG) called Full Duplex Radio Technology for Military Applications (IST-175) under the Information Systems Technology (IST) panel of the NATO Science and Technology Organization (STO).



(a) direct-conversion architecture



(b) radar-inspired architecture

Figure 2. Two architectures for implementing a full-duplex transceiver [1].

4.1. Groundwork for the research

We recorded the radio signals of all the aforementioned drone models (at both 2.4 GHz and 5 GHz) in the baseband IQ format and released the data online in a permanent open-access repository. For ourselves, the value of the dataset was to act as reverse-engineering material for understanding the physical-layer signaling and link-level protocols that drone systems employ for control and video transmissions. It can be noted that the radio signal database was concentrated on the market leader's models and, thus, we plan to extend it in later versions after new measurement campaigns.

We developed a full-duplex testbed for experimenting with detection and jamming efficiency against drones' RC links. Using the testbed, in [4], we then studied what is the most effective waveform for jamming a typical off-the-shelf RC receiver. As a case study, the targeted example system utilizes Gaussian frequency-shift keying control signal with frequency-hopping spread spectrum. The frame error rate of the receiver was measured with varying jamming power levels, based on which the successful identification of the most efficient waveform enables the jamming of the RC receiver with the least amount of power or at the longest distance possible. The study was continued in [6], where the self-interference cancellation performance of typical jamming waveforms is experimentally measured, and signal detection is performed over samples with imperfect self-interference cancellation. Significant differences were observed between waveforms.

4.2. Full-duplex radio technology

We proposed a novel system concept that consists of full-duplex transceivers and uses a multifunction signal for simultaneous two-way communication, jamming, and sensing tasks [7]. The transceiver architecture developed in [1] and the waveform thereof enable simple-yet-effective interference suppression at the cost of being limited to constant-

envelope transmission — this is a weakness only for the communication functionality that becomes limited to frequency-shift keying while FMCW waveforms are inherently effective for jamming and sensing purposes. We showed how transmission and reception as well as different interference and distortion compensation procedures are implemented in such multifunction transceivers [7]; the system could be also applied for simultaneous spectrum monitoring with the above functions. Finally, we showcased the expected performance of such a system through simulations. In [9], the dual-function radar and data reception performance was verified through measurements.

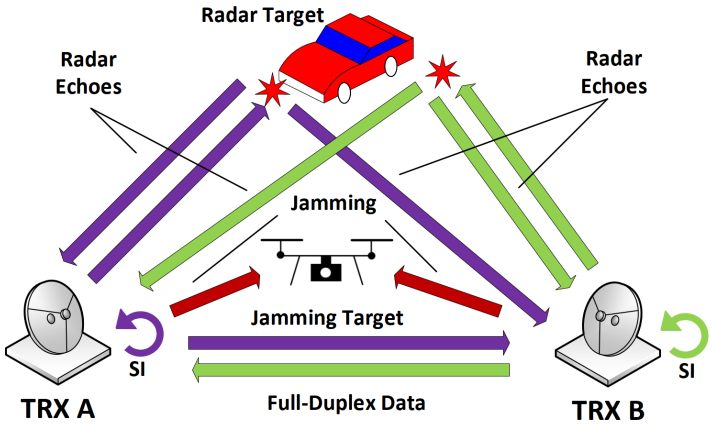


Figure 3. A concept picture of the proposed multifunction system [7].

4.3. Machine learning for counter-drone systems

In [3], we demonstrated the feasibility of simultaneous jamming and reconnaissance of drones' RC systems using a prototype full-duplex radio. Alongside, we applied deep learning in the form of a convolutional neural network for classifying the RC signals and analyzed the effect of full-duplex operation on the classification performance.

In general, efficient defense systems operate through multiple stages: detecting, locating, assessing, and eliminating threats. In [10], an overview of the most prominent methods belonging to those stages has been given along with discussions on how neural networks could improve them. Indeed, neural networks have already been shown capable of enhancing many of these methods, yet ample research opportunities remain open. The current counter-drone systems are far from invincible, but that is a worthy target to pursue, and we believe that neural networks are crucial to that end.

5. Conclusions

The research objectives were accomplished as planned. As the groundwork, we generated good understanding of drones' radio signals to be counteracted, jamming signals' performance against drones' control signals, and a full-duplex radio's performance for cancelling different jamming signals. The project introduced the new radar-inspired transceiver architecture to full-duplex systems. The results indicate that, due to efficient self-interference cancellation, the solution is especially promising for jamming applications, where restricting the transmitted signal to frequency modulation is not so challenging compared to communications. Secondly, the project clearly characterized the significant role of machine learning in developing counter-drone systems of the future. At these both areas, the project served as an important launch for our long-term research.

The objectives and outcomes of the project are coincidentally very much aligned with the scope of a new exploratory team (ET) called RF Finger Printing of Drones (IST-ET-120) under the NATO STO. According to the public online activity description, the ET aims to

"1. Evaluate the significance of a drone RF database. 2. Identify the promising RF detection, classification and localization techniques based on spectral information, including AI-based approaches. 3. Identify jamming techniques for soft neutralization. 4. Define test scenarios for drone detection, classification and localization in diverse environments. 5. Prepare the TAP [technical activity proposal] for the RTG." Thus, we recommend that the project's research work is continued through international collaboration within the ET and the anticipated RTG during the following years.

6. Scientific publishing and other reports produced by the research project

In chronological order, the research project's scientific publishing comprises two magazine articles, six conference papers, a master's thesis, and an online dataset as follows.

[1] J. Marin, Full-Duplex Transceiver Inspired by Frequency-Modulated Continuous-Wave Radar, M.Sc. (Tech.) thesis, Tampere University, April 2020.

[2] K. Pärlin and T. Riihonen, "Analog mitigation of frequency-modulated interference for improved GNSS reception," in *Proc. 10th International Conference on Localization and GNSS (ICL-GNSS)*, June 2020.

[3] K. Pärlin, T. Riihonen, G. Karm, and M. Turunen, "Jamming and classification of drones using full-duplex radios and deep learning," in *Proc. 31st IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, September 2020.

[4] J. Marin, M. Heino, J. Saikanmäki, M. Mäenpää, A.-P. Saarinen, and T. Riihonen, "Perfecting jamming signals against RC systems: An experimental case study on FHSS with GFSK," in *Proc. 31st IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, September 2020.

[5] M. Vuorenmaa, J. Marin, M. Heino, M. Turunen, and T. Riihonen, "Radio-frequency control and video signal recordings of drones," data set, *Zenodo*, November 2020.

[6] J. Marin, M. Turunen, M. Bernhardt, and T. Riihonen, "Self-interference cancellation performance in full-duplex jamming and spectrum monitoring," in *Proc. International Conference on Military Communications and Information Systems (ICMCIS)*, May 2021.

[7] J. Marin, M. Bernhardt, and T. Riihonen, "Full-duplex multifunction transceiver with joint constant envelope transmission and wideband reception," in *Proc. 46th IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, June 2021.

[8] K. Pärlin, T. Riihonen, V. Le Nir, M. Bowyer, T. Ranström, E. Axell, B. Asp, R. Ulman, M. Tschauner, and M. Adrat, "Full-duplex tactical information and electronic warfare systems," *IEEE Communications Magazine*, vol. 59, no. 8, pp. 73–79, August 2021.

[9] J. Marin, M. Bernhardt, M. Heino, and T. Riihonen, "Monostatic FMCW radar architecture for multifunction full-duplex radios," in *Proc. 55th Annual Asilomar Conference on Signals, Systems, and Computers (ACSSC)*, November 2021.

[10] J. Marin, K. Pärlin, M. Bernhardt, and T. Riihonen, "Neural networks in the pursuit of invincible counter-drone systems," *IEEE Potentials*, in press.

Publications [4] and [5] represent the groundwork for the research line. A direct-conversion full-duplex radio transceiver is used in [2], [3], and [6], while the radar-inspired architecture for a full-duplex radio is considered in [1], [7], and [9]. Machine learning for counter-drone systems is discussed in [3] and [10]. As an outcome of international collaboration within the NATO STO's research task group IST-175, the article [8] is a high-profile overview to the prospects of full-duplex radios in tactical communications and electronic warfare, where drones and their countermeasures are significant elements.