Neural Networks in the Pursuit of Invincible Counter-Drone Systems

Jaakko Marin, Karel Pärlin, Micael Bernhardt, and Taneli Riihonen

ⓒCarlos Baquero Barneto/Tampere University

(Our suggestion for an eye-catching cover photo — not referenced in the text)

The growing range of possibilities provided by the proliferation of commercial unmanned aerial vehicles, or drones, raises alarming safety and security threats. Efficient mitigation of these threats depends on authorities having defence systems to counter both accidentally trespassing and maliciously operated drones. To effectively counter such drones, the defence 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 (ML) could be the key for an endless improvement of counter-drone systems' techniques and abilities, providing them with an advantage that makes them virtually unbeatable in the field.

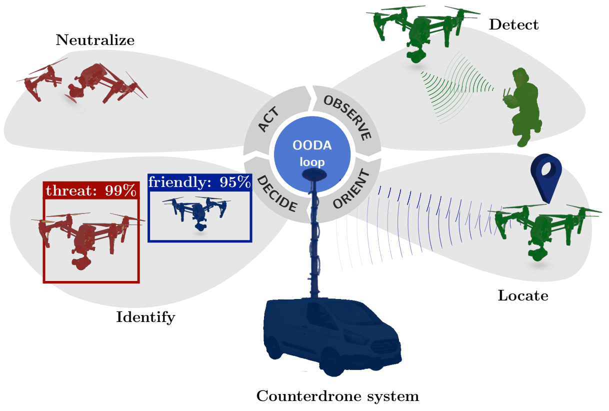

Fig. 1: Counter-drone operations illustrated through the observe–orient–decide–act (OODA) loop, which originates from the defence sector but fits to explain the counter-drone procedures also in civilian and commercial contexts.

ML already plays an important role in extracting relevant data from various sensors in computer vision and speech recognition, among other operations. Typically, ML systems rely on artificial neural networks (NNs) that have been vaguely inspired by biological NNs and are trained to relate some type of inputs to another type of outputs as illustrated in Fig. 2, by considering a vast number of examples instead of specifically programming explicit rules. Usually, a handcrafted algorithm is better optimized for any task than a NN. However, the learning ability of NNs can significantly relax the engineering workload that is otherwise required for solving problems with a large number of inputs and outputs, thus making the overall system design process more efficient. Additionally, NNs might be able to detect features in the data that an engineer might have missed or that are not perceivable for a human.

It is therefore not surprising that ML algorithms, and NNs in particular, 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, ML methods might prove crucial in aggregating data obtained from multiple sensors of different types through sensor fusion, which leads to enhanced situational awareness.

In this article, we discuss how NNs are used to enhance the four stages of drone mitigation, provide references to bibliographic surveys devoted to counter-drone security systems featuring NNs, and draw attention to potential research opportunities we envision in this field — hopefully

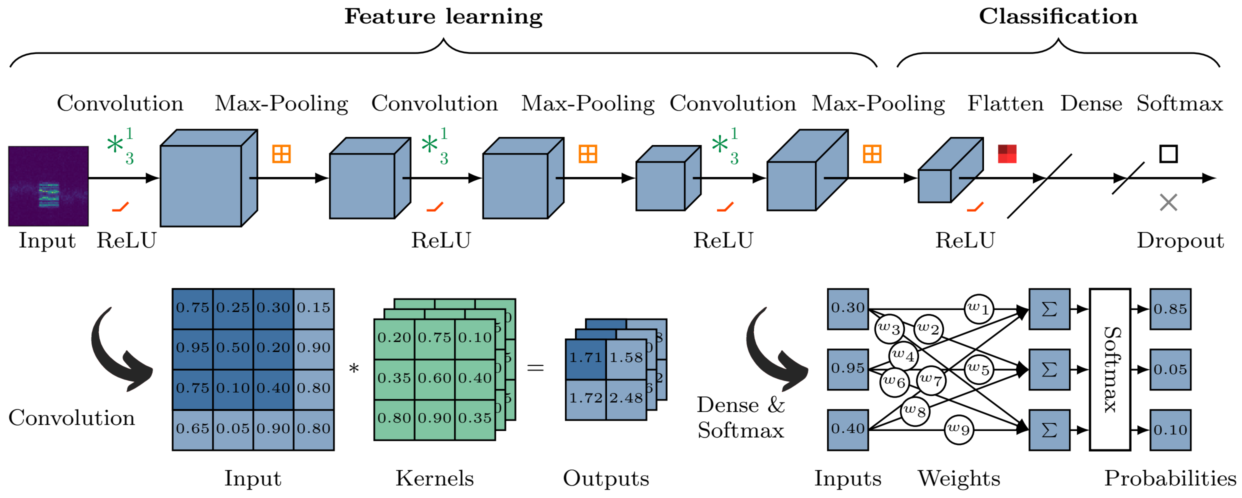

Fig. 2: An example of a convolutional neural network that we used in our earlier study on drone classification from radio spectrograms, together with illustrations on its basic building blocks.

spurring on forward-thinking students to participate in novel and high-impact research on NNs in counter-drone systems.

Detecting Drones

The first step towards risk assessment and mitigation is detecting the threatening drone. Detection can be performed in radio, radar, audio, or visual domains as illustrated in Fig. 3, because they typically rely on radio signals for communications with ground control, their moving rotor blades have distinguishable radar signatures, the rotors create an audible noise, and they become more visible as they approach the observer.

From these options, radio and radar typically offer the longest detection range. Furthermore, since radar signals need to travel both ways and small drones are weak radar targets, drones are typically detectable at even longer distances through radio signals than with radars. As a result, radio detection is often considered as the main method for drone discovery. However, if a target drone is completely autonomous and not transmitting anything, then detection needs to be performed in other domains.

Radio Detection

The goal of drone detection from radio data is to recognize and classify drone signals in the radio spectrum. A typical approach is to transform the received signals to a time–frequency

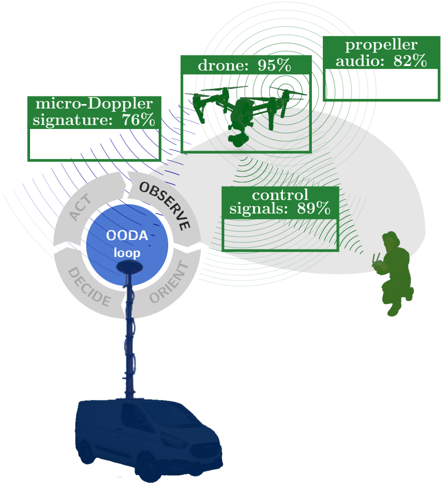

Fig. 3: Drone detection — a counter-drone system detects a new target using its radio analyzer, radar, microphone, and camera.

representation known as spectrogram, and then use NNs to detect and classify different signals from those images, similarly to how NNs are used for object recognition from photographs in computer vision.

However, radio spectrograms are inherently complex-valued entities, which calls for revising the conventional methods that operate on real-valued color photographs. One approach, although not yet as well studied, is to use complex-valued NNs directly on the received signals. This way, intrinsic information potentially available in both amplitude and phase of the signal can be leveraged for detection purposes. Further research should be done into developing complex-value-based NNs and studying their benefits and performances at different tasks.

Overall, recent experiments have shown good performance when using NNs to detect and classify the drone models from a radio signal. Detecting drones from radar signals also falls under this category. However, as radars inherently include ranging, this is covered in more detail in the next section on locating and tracking drones.

Video and Audio Detection

ML has been leading the way for computer vision and speech recognition solutions for some time. Therefore, as would be expected, NNs show promising results in both video- and audio-based drone detection as well — NNs are capable of detecting and classifying between numerous different types of commercial drones with very high accuracy based on just visual or audio data.

A disadvantage in video- and audio-based methods is that they are expected to be adversely affected by environment conditions, such as weather and urban noise. However, these methods are essential to developing robust counter-drone systems that can handle radio-silent operations or drones that use wireless communications that are not typically characteristic to them, such as mobile networks. Additionally, vision-based methods provide an easy way for human operators to interpret and understand the threat situation.

Research Opportunities

Drone detection from different sensors using NNs is a relatively well researched topic. Furthermore, NNs have been reported to achieve high accuracy even when a large variety of consumer drones have been used during the training phase. However, the detection of drones outside of the learning dataset, especially with radio signals, is an open research question — how to detect and classify drones that use unknown signal types in a crowded radio spectrum? This is especially important, since new signal protocols with diverse uses are developed rapidly. Would such signals get classified incorrectly as another drone or be discarded as noise?

LOCATING AND TRACKING DRONES

After detecting an appearing drone, finding out its geographical location and subsequently tracking its movements becomes important to assess the potential threat that the drone poses, and to support identification and neutralization of the drone as illustrated in Fig. 4.

Similarly to drone detection, locating and tracking of drones can be based on various sensors, ideally relying on sensor fusion for best results. However, locating and tracking operations do not often rely on NNs, since these operations are quite well established and do not involve any immediately intuitive classification problems. Regardless, several examples of using NNs for improving accuracy and performance have been reported.

Radio and Radar Localization

When countering malicious drones, it is often essential to locate not only the drone itself, but also the drone operator. In most conditions, radio-based sensors provide the most straightforward, if not the only, option for tracking both the drone and its remote control operator.

Locating radio signal sources is typically achieved by combining multiple direction-of-arrival (DoA) detectors into a triangulation system, or by combining multiple time-synchronized sensors

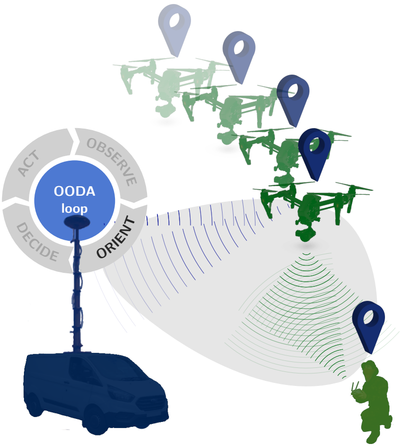

Fig. 4: Drone localization and tracking — often it is also essential to locate the drone operator.

into a time difference-of-arrival (TDoA) system. It is also possible to use a single DoA detector together with a path-loss model and knowledge about transmitted signal power to estimate the distance of the transmitter from the received signal's power. If the sensor's receiver does not have a line-of-sight to the transmitter, then the accuracy of these methods are usually quite poor.

Several works have considered the use of ML for simplifying the implementation or improving the accuracy of locating and tracking radio emitters. This is especially important, as conventional DoA estimation algorithms, such as MUSIC, are computationally expensive. As such, NNs have been applied for estimating the direction of a radio emitter from noisy measurements with notable accuracy by employing even a single DoA detector. It is also noteworthy that radio-based drone locating methods are amongst the leading candidates to be used in counter-drone unmanned aerial vehicles. That is because elevating radio sensors can significantly improve their performance when locating and tracking drones, especially in urban scenarios.

A drone's micro-motions impart changes to radar echo signals and since targets with differing physical builds, such as different drone models, each have micro-motions which are characteristic to that build, those changes to radar signals become distinguishable and are called micro-Doppler signatures. Classifying these signatures is especially suitable for NN applications.

However, NNs also have the potential to aid modelling drone movement and thus tracking the drone. Initially, Kalman filters were designed for tracking single targets and revolutionized this area by providing the possibility to use complex tracking models. More recently, NN-based methods have been proposed for handling maneuvering targets or multiple targets with clutter.

Such NN methods have the potential to become a key enabling technology for cognitive radars to track and predict the movement of multiple drones. As a testament to that, NNs have been considered for collision avoidance on-board of drones in order to avoid other aircraft.

Video and Audio Localization

Visual tracking is one of the most prominent topics in the field of computer vision, wherein the goal is to automatically estimate the states of the target object in the subsequent frames. Recently it has been shown, that conventional particle filter and sliding window-based motion models can be outperformed by NN-based motion models for trajectory prediction in visual tracking applications. Similarly, it has been shown that NN implementations are able to accurately track suspicious airborne targets and even combine feeds from multiple cameras to track a single target. After all, NNs have already been proposed for controlling the movements of drones and it is natural to use the same technology to anticipate their behavior.

Propeller sound coming from the drone can be used in a similar way as with radio-based methods to extract location and track movements of a drone. The benefit of audio-based methods compared to radio-based ones is arguable, but sensor fusion is useful in scenarios with strong interference or when the target does not transmit radio signals.

The main weakness of the audio-based approach is that the propellers of the drone are usually rather quiet and the ambient noise present in any real environment can easily mask the sound of the drone from any meaningful distance. Yet, drone DoA estimation using acoustic arrays is an interesting topic and similarly to radio-based DoA estimation, NNs can be exploited for improved pinpointing of acoustic sources in noisy conditions.

Research Opportunities

From a security point of view, one of the most alarming developments considering the rapidly evolving capabilities of drones is their ability to operate in a completely autonomous way. For counter-drone purposes, this will make detecting and locating the drone and its operator using radio-based methods more difficult if not impossible, as the drone will not require continuous communication with the operator. It has already been shown that using multiple camera feeds to track a single drone using NNs is feasible. However, can NNs be extended to take advantage of sensor fusion and track a drone not only from multiple same type sensors but using sensors of completely different types? For example, would combining thermal imaging and regular cameras help overcome some of the weather induced difficulties in visual tracking?

IDENTIFYING DRONES

After detecting and locating a drone in the area, it becomes essential to assess the risk that the drone poses. It has been proposed that all drones are required to carry a transponder that transmits the drone's and its owner's information, such as the drone's location, licence number, and the owner's name and contact information. Thus, if a drone is flying with its transponder off, it could be immediately classified as a potential threat or a malfunctioning transponder. Alternatively, if a drone with an active transponder is unknowingly approaching a restricted area, its owner could be contacted and the risk mitigated. However, other methods of extracting useful information from non-cooperative drones exist as shown in Fig. 5.

Transmitter Chip Identification

In signal classification field, NNs have proven to be able to recognize and categorize different signal modulations and communication protocols. This information could potentially be used to identify the radio chip models, which are used by the drone and its remote controller.

Various drones might be constructed using the same chipset, so knowing the protocol is not necessarily enough information to identify the drone model. However, knowledge about the specific components used in the advancing drone obtained from several sensors, sources, or algorithms, can be combined and used in a database search to evaluate the drone's capabilities (e.g., transmitter output power, flight speed, payload capacity) and thus assess the risk posed by the drone, or assist in locating and tracking the drone.

Radio and Radar Fingerprinting

In any radio transmitter, the analog electronics components within the signal transmission path (e.g., digital-to-analog converters, band-pass filters, frequency mixes, and power amplifiers) have slight imperfections that impose unique distortions on their transmit signals. Numerous works have studied the possibility of fingerprinting various radios (e.g., WiFi and Internet-of-Things devices) based on those imperfections from a device population of hundreds to thousands of devices using NNs. The results from these works have been highly encouraging, as NNs have been shown capable of identifying specific radios from moderately large device populations based

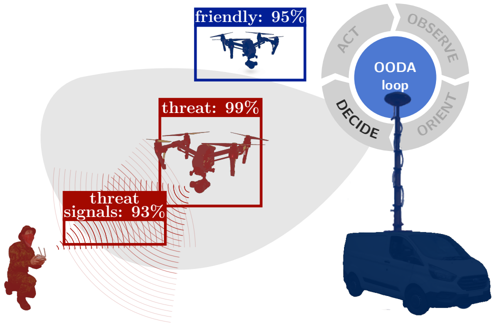

Fig. 5: Drone identification — the threat level and affiliation of the drones is determined based on extracted information.

on the hardware imperfections. However, such identification accuracy depends on the signal-to-interference-plus-noise ratio of the received signal and the distortions caused by the wireless channel, including all elements in the signal path from source to destination.

Radar-based identification is based on the unique distance–Doppler profile generated by the drone and its different moving parts. Such methods can be used to discover the number of propellers, their length and rotation speed. It might be possible to acquire the radar cross section, as well as whether the drone is carrying a payload. Consequently, such information can be used to estimate the drone model, but if various models share the same characteristics, it can lead to ambiguity. Regardless, the drone class can be estimated from this information.

Audio and Video Profile Identification

Speaker recognition has been studied for long before drones became a security concern and ML approaches are successful at recognizing individual speakers from audio. More recently, NNs have also been successfully applied for distinguishing drones using the acoustic signatures that the rotors generate. This solution seems to provide good identification performance, but since the drones are not very loud and the noise situation can vary drastically, the range and reliability of this method can be quite poor.

Image processing with NNs can also give a definite answer about the specific model of the drone, as well as whether it conveys a payload and of which size (e.g., if the drone is carrying a camera or an explosive device). However, for visual identification methods to work, the drone must be in clear line-of-sight view from the camera, which limits the method's coverage and functionality in adverse environmental conditions.

Research Opportunities

Drone identification will be essential when distinguishing between drones belonging to regular users, law enforcement, and malicious users. As such, accurate identification could be used to determine the threat posed by a drone, or even as forensic evidence in hindsight. NNs are already showing good results in identification tasks.

However, perhaps the biggest challenge for NN-based identification is scalability. What kind of NN architectures are required to identify specific units amongst very large device populations — what are fundamental limits of robust fingerprinting? Also, what kind of impact will realistic channels have on identification accuracy, how to overcome those channel effects, and can such identification methods be guaranteed to be non-cheatable? Another open question is if NN-based methods can also be used to identify the threat carried by the drone, e.g., whether the drone is carrying a surveillance camera or an explosive device?

NEUTRALIZING DRONES

After a drone has been identified as a potential threat, the risks it poses need to be minimized. The possibilities range from aggressive methods, like firing projectiles or nets, to more subtle methods, like control channel or satellite navigation jamming. A visualization of the latter can be seen in Fig. 6.

The concept behind jamming is to transmit a powerful signal in the same frequency band as the one used by the drone, making it difficult for the drone to demodulate the signal it is receiving. Most of the public research is concerned in detecting and mitigating jamming using NNs, whereas research into leveraging NNs for jamming is limited. However, several aspects of improving jamming through ML can be and indeed have been considered.

Waveform Adaptation

The signal waveform used for jamming the drone's remote control or satellite navigation receivers has a great impact on the jammer's performance. Therefore, the jamming waveform is a prime candidate for modification to increase efficiency. The adjustable parameters could be the center frequency, bandwidth and idle time of a noise-type signal.

Should the jammer be able to observe the drone's response to jamming, adjusting the jamming waveforms parameters accordingly can be considered as a reinforcement learning operation, for which NNs are well suited. By using ML, a jammer that does not have any prior knowledge

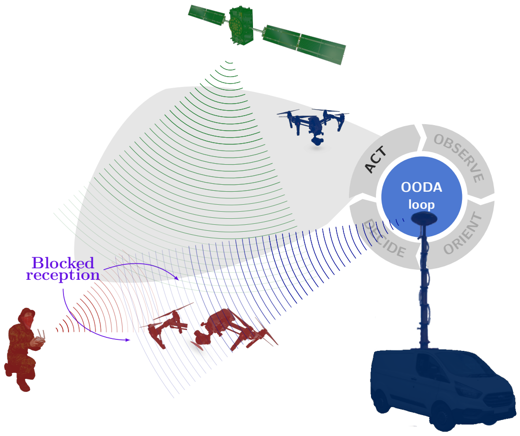

Fig. 6: Drone neutralization — NN-enhanced waveform and transmitter power adaptation together with beamforming can reduce collateral damage.

about the transmitter's algorithm, can effectively reduce or deny the transmitter's throughput compared to random or even sensing-based jamming.

Transmit Power Adaptation

In addition to adapting the waveform, it can also be advantageous to modify the transmitted jamming power. The idea is to minimize the power of the transmitted signal to a level where the jamming just works and the defence system transmits the least amount of energy needed to disable the target device.

Transmit power minimization is important to mitigate the collateral damage caused by the operation to nearby authorized actors using the same frequency band, as well as to hide the jamming operation from others, and to simply conserve energy. Similarly to modifying the waveform through reinforcement learning, the transmit power could be adapted to changing conditions in the scenario as a function of the perceived jamming efficiency.

Adaptive Beamforming

To further limit the unwanted collateral damage caused by jamming, and to increase power efficiency, the radiation pattern of the jamming antenna should be aimed to direct the signal only at the targeted drone(s). Beamforming can be performed by adjusting a directional antenna with electric motors, or through signal processing with an antenna array. For beamforming to be effective, the location of the drone needs to be accurately known.

In previous sections, we have already discussed how various sensors enhanced with NN-based methods can be used for locating and tracking drones. Such systems are essential for directing the jamming energy towards the targeted drone. A NN could be given a task of deciding inputs to classic beamforming algorithms, or to directly adapt the antenna element weights, but whether such a system brings any meaningful benefit over traditional methods is an open research question.

Research Opportunities

A jammer equipped with artificial intelligence could maximize the jamming performance while minimizing the collateral damage caused by it, and even more so if so-called full-duplex radio technology was used to enable simultaneous radio transmission and reception. It might even be possible to hijack a flying drone by utilizing a learning jammer that mimics the control signaling or GPS while observing the drone's movement, thus moving it away from a critical location.

Surprisingly or not, the rapid rise and dependence on NNs in drone applications themselves might open another trail for countering them, should some forward-thinking researcher explore it. Despite its enormous success in many computer vision, signal classification, and signal tracking applications, ML itself is exceedingly vulnerable to adversarial attacks. For example, radio signal modulation classification performance can be significantly reduced even with small perturbations of the input signal. As such, these adversarial attacks can be significantly more powerful than classical jamming attacks, which raises security and robustness concerns in the use of ML algorithms for wireless physical layer. It is plausible that as NN-based applications find more use in drones, the counter-drone solutions will benefit from targeting the underlying NNs.

Conclusion

Rogue consumer/prosumer drones pose a significant threat to both civilian and military security and therefore need to be counteracted with efficient defence systems. Such systems need to operate through multiple stages: detecting, locating, assessing, and eliminating threats. In this article, 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, however, that is a worthy target to pursue and we believe that neural networks are crucial in its realization.

Read more about it

- G. Ding, Q. Wu, L. Zhang, Y. Lin, T. A. Tsiftsis, and Y.-D. Yao, “An amateur drone surveillance system based on the cognitive Internet of Things,” *IEEE Communications Magazine*, vol. 56, no. 1, pp. 29–35, Jan. 2018.
- M. M. Azari, H. Sallouha, A. Chiumento, S. Rajendran, E. Vinogradov, and S. Pollin, “Key technologies and system trade-offs for detection and localization of amateur drones,” *IEEE Communications Magazine*, vol. 56, no. 1, pp. 51–57, Jan. 2018.
- M. Sadeghi and E. G. Larsson, “Adversarial attacks on deep-learning based radio signal classification,” *IEEE Wireless Communications Letters*, vol. 8, no. 1, pp. 213–216, Feb. 2018.
- I. Guvenc, F. Koohifar, S. Singh, M. L. Sichitiu, and D. Matolak, “Detection, tracking, and interdiction for amateur drones,” *IEEE Communications Magazine*, vol. 56, no. 4, pp. 75–81, Apr. 2018.
- B. Taha and A. Shoufan, “Machine learning-based drone detection and classification: State-of-the-art in research,” *IEEE Access*, vol. 7, pp. 138 669–138 682, Sep. 2019.
- S. Samaras, E. Diamantidou, D. Ataloglou, N. Sakellariou, A. Vafeiadis, V. Magoulianitis, A. Lalas, A. Dimou, D. Zarpalas, K. Votis, P. Daras, and D. Tzovaras, “Deep learning on multi sensor data for counter UAV applications—a systematic review,” *Sensors*, vol. 19, no. 22, p. 4837, Nov. 2019.
- G. Lykou, D. Moustakas, and D. Gritzalis, “Defending airports from UAS: A survey on cyber-attacks and counter-drone sensing technologies,” *Sensors*, vol. 20, no. 12, p. 3537, Jun. 2020.
- K. Pärlin, T. Riihonen, G. Karm, and M. Turunen, “Jamming and classification of drones using full-duplex radios and deep learning,” in *Proc. 31st Annual International Symposium on Personal, Indoor and Mobile Radio Communications*, Aug. 2020.
- H. Kang, J. Joung, J. Kim, J. Kang, and Y. S. Cho, “Protect your sky: A survey of counter unmanned aerial vehicle systems,” *IEEE Access*, vol. 8, pp. 168 671–168 710, Sep. 2020.
- Y. E. Sagduyu, Y. Shi, and T. Erpek, “Adversarial deep learning for over-the-air spectrum poisoning attacks,” *IEEE Transactions on Mobile Computing*, vol. 20, no. 2, pp. 306–319, Feb. 2021.
- J. Wang, Y. Liu, and H. Song, “Counter-unmanned aircraft system(s) (C-UAS): State of the art, challenges and future trends,” *IEEE Aerospace and Electronic Systems Magazine*, vol. 36, no. 3, pp. 4–29, Mar. 2021.
- 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, Aug. 2021.

About the authors

Jaakko Marin (jaakko.marin@tuni.fi) earned his M.Sc. degree from Tampere University, Tampere, Finland. He is a doctoral researcher at Tampere University, Tampere, Finland.

Karel Pärlin (karel.parlin@rantelon.ee) earned his M.Sc. degree from Tallinn University of Technology, Tallinn, Estonia. He is an engineer at Rantelon, Tallinn, Estonia.

Micael Bernhardt (micael.bernhardt@tuni.fi) earned his Ph.D. degree from National University of the South, Bahía Blanca, Argentina. He is a postdoctoral researcher at Tampere University, Tampere, Finland.

Taneli Riihonen (taneli.riihonen@tuni.fi) earned his D.Sc. degree from Aalto University, Helsinki, Finland. He is an assistant professor at Tampere University, Tampere, Finland.

ACKNOWLEDGMENT

The work leading to this publication was funded in part by the Finnish Scientific Advisory Board for Defence, the Academy of Finland, the Estonian Ministry of Defence, and the EDA Defence Innovation Prize.