

JUNE 2020 ISSUE NO. 370

Developing an Effective Anti-Drone System for India's Armed Forces

VIVEK GOPAL

ABSTRACT The use of drones or Unmanned Aerial Vehicles (UAVs), both for military and civilian purposes, has increased in India in the past decade. At the same time, counterdrone systems are also being developed to address the threats posed by UAVs. How effective are these counter-drone mechanisms? This brief explores this question, and offers suggestions for India to reduce the growing threat from drones. Any evaluation of the efficacy of anti-drone systems has to be conducted in view of current technologies such as Artificial Intelligence (AI), cognitive Global Positioning System avoidance, and hardware sandboxing—and such is the aim of this brief.

Attribution: Vivek Gopal, "Developing an Effective Anti-Drone System for India's Armed Forces," *ORF Issue Brief No.* 370, June 2020, Observer Research Foundation.

Observer Research Foundation (ORF) is a public policy think tank that aims to influence the formulation of policies for building a strong and prosperous India. ORF pursues these goals by providing informed analyses and in-depth research, and organising events that serve as platforms for stimulating and productive discussions.



INTRODUCTION

In the past several years, India has been seeing more use of drones—or small unmanned aerial vehicles (UAVs)—for various military and civilian purposes. These include reconnaissance, imaging, damage assessment, payload delivery (lethal as well as utilitarian) and as seen recently amidst the COVID-19 pandemic, for contact-less delivery of medicines. The use of drones, however, poses threats to public security and personal privacy.1 Analysts warn that as Unmanned Aerial Systems (UAS) become less expensive, easier to fly, and more adaptable for crime, terrorism or military purposes, defence forces will increasingly be challenged by the need to quickly detect and identify such aircraft.2 The Small Unmanned Aircraft System (sUAS) technologies are continuously evolving: indeed, customised UAVs, micro sUAS—i.e., UAVs. drones with their controller stations and equipment—can operate without radio frequency (RF) command and control links, and can use automated target tracking, aside from having obstacle avoidance and software-controlled capabilities.³

This brief outlines the significance of the various threats posed by the increasing use of drones. It suggests a roadmap for addressing such threats. The brief covers the aspects of detection, identification and localisation techniques, as well as jamming and other countering measures. It also looks into the various existing anti-UAS solutions already in the market.

DETECTION, IDENTIFICATION AND LOCALISATION TECHNIQUES

Drones have low Radar Cross Section (RCS), slow speed and a small size—these characteristics make the task of detection difficult, and thereafter, identification and localisation even more so. In response, governments and military forces across the world, including in India have developed various approaches to detect these aerial systems. These methods can broadly be classified as radar, video/electro-optical (EO), audio/acoustic, and RF-based.

Detection Techniques

Radar. Radar is a useful tool for detection of aircraft. There are various challenges, however. These include a drone's low altitude and velocity of flying, and very small radar cross-section (RCS) which makes it extremely difficult to distinguish noise or clutter from the actual target.

RCS Study. Analysing the micro-doppler signature by multi-static radar can help in accurate drone detection and tracking. ⁴ Small drone RCS estimation obtained by outdoor measurements has been analysed and proved that passive techniques can be used to detect and track drones. ⁵ Back scattering phenomenon associated with micro motion has also been studied by scientists. Whereas the total RCS is important for target detection, the energy backscattered from rotating parts like propeller and rotors are crucial for extraction

of useful micro-Doppler signatures.a

Multiple Input Single Output (MISO) Radar Systems. A single antenna is used for transmission, whereas four antennae are used for reception. The concept of estimating the minimum power requirement that must be transmitted to reveal a target with a specific value of RCS is possible with the radar equation. Drones up to a range of 150 metres can be detected using this technique.⁶

Multiple Input Multiple Output (MIMO) Radar Systems. Using MIMO radar systems further increases the probability of detection of drones and UAVs. It introduces high angular resolution and sensitivity for slowmoving targets and covers a wider area with lesser cost, as compared to conventional phased array systems. It also exhibits enhanced discrimination from clutter and phase noise.⁷

Ku-Band (12 Giga-hertz) to **18** Battlefield Radars. Theoretical analysis of the detection probability has been carried out ⁸ in addition to the relationship between signal to noise ratio as well as small RCS of drones. This was based on a study sponsored by MoD of the Slovak Republic. A 35 Gigahertz Frequency Modulated Continuous Wave (FMCW) drone detection system has also been studied, and the results obtained have been validated in theory as well as practice.9

Classification and Localisation Techniques

Audio. Although not a highly effective system in the stand-alone mode due to the omnipresent background noise which increases the complexity of detection and computation, it can be used as a system that can be superimposed with other detection techniques. During the flight of the drone, the sound generated by the rotors can be utilised in detection, classification and localisation of drones. Algorithms such as Multiple Signal Classification (MUSIC) can be used to estimate the direction of arrival. Tetrahedron acoustic arrays have been used in systems to find out the direction of arrival using received signal strength and time difference of arrival method in addition to Kalman filter for tracking. 10, 11

Optical/Video/Infrared (IR). An object can be detected based on its appearance features and/or its motion features across consecutive frames. For drone detection, it is promising to combine both motion features and appearance features—this gives higher accuracy to the system. A thermal imaging-based enhancement algorithm for IR scanner system has also been proposed by the Military Institute of Technology, Poland. Even in conditions of low visibility, the IR spectrum can be discerned at considerable distances. However, there are certain disadvantages with IR systems, including: low spatial resolution, low

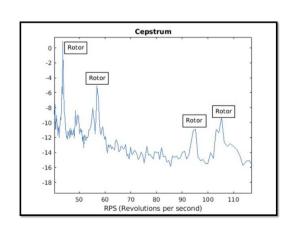
a Demirev V., 2017, "Drone Detection in Urban Environment – The New Challenge for the Radar Systems Designers", International Scientific Journal "Security & Future", WEB ISSN 2535-082X, Year 1 Issue 3, pp 114-116.

image contrast, diffused edges, presence of noise, and pulse disturbances. The Inverse Synthetic Aperture Radar (ISAR) technique has also been employed during a study in Korea Aerospace Research Institute, for counter UAS systems to detect drones in urban areas. The detailed structure, size of the drone and the number of rotors can also be determined using this technique of ISAR as demonstrated in the study.¹⁵

Micro-Doppler Analysis. The doppler signature depends on parts of an object moving and rotating in addition to the main body motion (e.g. rotor blades) and is a characteristic of the type of object. Research has been centred around understanding the micro-doppler spectra of specific commercial drones whose rotor blades or hubs are uniformly displaced from the platform centre of mass. When superimposed with radars in the X-Band (7-11 Giga-hertz) and Ku-Band, there is higher accuracy due to the fusion of the radar sensor data as compared to a single radar. 16,17 The cepstrum reveals, using signal processing techniques, how the received signals can be used for image recognition. As shown in Figure 1, the study carried out at Fraunhofer Institute for High Frequency Physics and Radar Techniques (FHR), Germany, micro-Doppler analysis when used in conjunction with radar data, provides good results when determining the rotational speed of the rotors. The individual rotor speeds can subsequently be read from the cepstrogram or the cepstrum. The accompanying graph shows the cepstrum of the four rotor blades of a drone flight. Due to the flight movement of the drone, two of the blades are rotating faster, therefore the higher rotations per minute. Principal Component Analysis (PCA) is another method used to reduce the number of variables in data by extracting important ones from a large pool. It reduces the dimension (size) of the data with the aim of retaining as much information as possible. The PCA technique has been used for feature extraction from time-frequency spectrograms in addition to support vector machines (supervised machine learning algorithms) to recognise the drones.

Fig.1- Micro-doppler Radar DroMiAn (Drone detection with micro-Doppler Analysis) (Left) & Cepstrum of Four Rotor Blades (Right)





(Image Source: https://www.fhr.fraunhofer.de/en/businessunits/security/Drone_detection_with_micro-doppler_analysis.html)

JAMMING AND COUNTERING TECHNIQUES

Defeating a drone can involve a plethora of techniques. To name a few, it may involve kinetic means, electronic warfare (EW) and cyber warfare (CW) techniques, Drone vs drone, and Directed Energy Weapons (DEW) using high-powered microwave or LASERs. Various integrated solutions have been offered in the world market with respect to defeating drones or sUAS. The noteworthy options include RF jamming, GPS jamming, GPS spoofing, and net guns. 18 While jamming the controller link is an option, the widely used concept involves jamming the GPS link (bands L1 to L5) to make the drone lose control of its "auto-home" option when the main controller link fails (i.e., jammed). One can also develop techniques to jam the payload WiFi link which will also be in almost the same frequency range as the 5 Giga-hertz controller link (HP 47 counter UAV Jammer does exactly this by blocking the video feeds). A layered approach is what will be preferable in a counter-drone system.

Boeing demonstrated the High Energy Laser Mobile Demonstrator in 2014, which fired a 10-Kilowatt LASER and could function effectively in different climatic conditions like rain, fog or wind. The Drone Catcher Gun is also a scalable option available to safeguard facilities as has been researched and demonstrated. The jamming of drones can also be effected using a 3D MIMO radar. By using directional antennae, the power is confined spatially, thereby allowing its use without interference to co-located RF devices/equipment.

The two most potent and comprehensive repositories of counter-UAS have been studied as part of preparing this brief. 21, 22 The resulting database as part of the aforementioned repositories is based on open-source research of technical and policy reports, news analyses, manufacturers' information, interviews with government officials, subject matter experts, and participation in conferences. The sheer volume as well as the description of the counter UAS weapons prohibits its inclusion in this brief.

The database consists of nearly 537 systems, sold by 277 vendors and fielded by 38 different countries, some alone and others as part of joint ventures between two nations. RF & radar detection have been found to be the most common detection techniques, followed by EO/IR systems. Jamming the RF and GNSS signals is the most common method, followed by a few which have spoofing capability. Some also mention the use of a 'sacrificial drone', or a drone that may be used to deliberately collide with the detected enemy drone to destroy it.

ARCHITECTURE AND IMPLEMENTATION

Of the 537 systems discussed earlier in this brief, unfortunately, none of the systems from India find a mention. This may be because information may be classified, or there was no participation by Indian vendors. However, during the Republic Day parade in 2020, there were media reports of an anti-drone weapon having been fielded.²³ Based on the various proof of concepts as well as technology

demonstrators, one can now elaborate on the system design for a modular counter-drone weapon. The main purpose of these measures is to exploit the vulnerabilities of drones.²⁴

Heterogenous Sensing Unit – Detection, Localisation and Tracking

A heterogenous sensing unit will serve the purpose of detection and localisation of the drone. The heterogenous system will comprise of various sensors which can be utilised in any weather. There should be RF/ radar-based sensors as the first line of detection, coupled with acoustic sensors. This can be followed by an EO/IR system layer for enhancing the resolution. The range of detection should be a minimum of three km and it should effectively be able to track the drone at minimum 1 km, assuming the drone is carrying a destructive payload.

Central Processing Unit

The Central Processing Unit should be able to collate the feed from all the active and passive sensors. It should thereafter carry out analysis, derive drone features, and achieve classification.

For the acoustic sensors, the Short Time Fourier Transform (STFT) can be adopted and the histogram of oriented gradients (HOG) can be used ²⁵ for extraction of image features. These are in addition to the PCA methods described earlier.

In the case of the RF features to be extracted, it may be assumed that at least two out of the following three links are active at any given point in time, viz., controller link or the ground control link (to include all frequency bands as prevalent based on the manufacturer specifications); GPS link (uplink & downlink frequency bands as also to cover GLONASS, Bediou & possibly IRNSS); and the payload (assumed camera/ optical device for reconnaissance) WiFi link back to the ground control station which may transmit the data captured in real time to the control station. The development and incorporation of neural networks can be considered subsequently. By using the logical 'OR' operation, it will be ensured that probabilities of detection are high despite the possibility of a false alarm, albeit to a minimum.

Jamming Unit

Based on the inputs and analysis carried out by the Central Processing Unit, the jamming unit can be made to work in three modes akin to air defence systems viz., Weapon Hold, Weapon Free, and Weapon Tight. Based on directional antennae to achieve better spatial economy as well as meet power requirements, a 360-degree coverage is preferable (gimbal^b based for added stabilisation) with a slaved servo/proportional-integral-derivative (feedback based) controller to the tracker. A spoofing unit should be made alongside the jamming unit to take over the drone if

b The word "gimbal" is defined as a pivoted support that allows rotation of any object in a single axis. So a three-axis gimbal allows any object mounted on the gimbal to be independent of the movement of the one holding the gimbal. The gimbal dictates the movement of the object, not the one carrying it.

desired for forensics at a later stage (Man in the middle attack^c).

Kill Unit

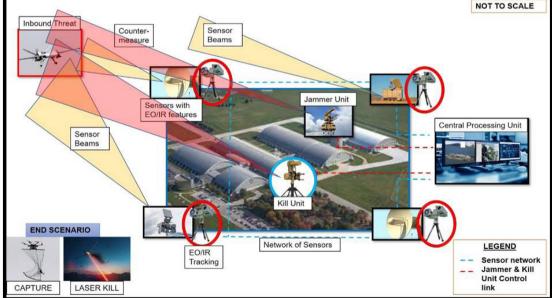
If the jamming unit is unable to affect the drone operations due to any reason, the highpower microwave unit should kick into action to get the drone on the ground. The range of engagement can be fixed with respect to various vulnerability aspects, such as the installation being defended, the importance of the area, and the vital point. An alternate high-power LASER may also be employed to destroy the drone. The close-in weapon support systems (CIWSS) as used extensively by naval vessels the world over against hostile missiles is also another option which may be explored.

System Integration and Implementation

The proposed system should be fabricated in a modular fashion allowing sub-system integration based on the felt need. The system at the same time should be made in two versions, viz., manpack (portable) and vehicle-based, obviously scaling down the parts and therefore, weight for the manpack system (SWaP considerations). The design of the system may be adapted from the system as shown in Figure 2.

Inbound/Threat Counter-Sensor

Fig. 2 Envisioned Counter Drone System - Layered Architecture



Author's own.

A man in the middle (MITM) attack is a general term for when a perpetrator positions himself in a conversation between a user and an application—either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway. A spoofed signal in the case of a drone will impersonate the actual signal of interest and misguide it.

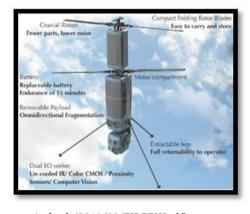
While the system as envisioned in this brief has been trial-evaluated, stakeholders in the anti-UAS campaign such as Rafael (Israel-based) have come up

with the Drone-DomeTM drone detection, neutralisation and interception system as well as the FireflyTM miniature tactical loitering weapon. d

Fig. 3- Drone Dome Brochure (Open Source) - Array of sensors and integration



Fig. 4- Firefly Brochure (Open Source) - Tactical loitering weapon to 'Kill' Drones



 $(Image\ Credit:\ https://www.rafael.co.il/wp-content/uploads/2019/03/FIREFLY.pdf)$

d A miniature EO tactical loitering munition which serves as ears and eyes for behind cover/ beyond line of sight. This capability as seen, may be exploited against drones also using its stand-off range as well as enhanced camera capability.

While the man-portable systems should be capable of being used by the dismounted soldier or the infantry, the vehicle-based system may be utilised to guard static installations. It is recommended that being a tri-service requirement, the fabricating process be undertaken under the aegis of the HQ Integrated Defence Staff or a prototype be developed as an Army Technology Board project. What must also be noted is that collaboration (internal civil industry as well as global players) in this field will reap greater dividends rather than a purely 'Make in India' approach which may take more time.

Under the gambit of the draft DPP 2020, the innovation scheme under the 'Make' category/ Innovation in Defence Excellence (iDEX)/ Technology Development Fund initiatives may help in the long run. DGCA will need to be incorporated to streamline the rules of engagement (Civil Aviation Requirements or CAR). Such 'Aerial Threat Reduction Teams (ATRT)' should be a triservices unit or outfit, with a participation by personnel from all three services, for effective and efficient utilisation.

CHALLENGES

This threat is evolving every three to six months—it is just that adaptive. This is going to be a continuing challenge due to the adaptive nature of the problem of being able to use small drones in so many different ways and you cannot rely on one technique to respond to them.

- Vayl S. Oxford, Director, U.S. Defence Threat Reduction Agency, March 2019.

The challenges being faced today with counter-drone to technology manifold drone technology is as growing by leaps and bounds. Reconnaissance, Intelligence, Surveillance & Target Acquisition (RISTA) & Electronic Warfare systems will have to work together to tackle the threat of both stand-alone and drone swarms. Some of the pertinent technologicalchallengesarebeinghighlighted which will need immediate attention to be considered when the anti-drone weapon is conceptualised.

Heterogenous Sensor Fusion. The variety of protocols used for communication between sensors poses a problem during their integration into a networked system.

Energy Efficient Sensors. Power management considerations will always be towering as the employment of such systems is going to be all-day and all-night. Solar power sources and fuel cells are the technologies which may be tapped.

Multiple Drone Detection and Localisation. Technical challenges will be compounded when trying to detect and localise swarms wherein it will not be necessary that all the drones are having a viable RF signature. Progress has been made in using millimetre -wave radar as well as measuring the turbulence caused by the drone rotors.

Drone Signature Database. Extensive studies are to be conducted to have a comprehensive database. Inter-agency cooperation may help mitigate the issues involved.

Identification Friend or Foe (IFF). The IFF shall always remain challenging with the use of drones for all unethical purposes by non-state actors. However, research has been carried out in this field using a relay drone with beacon system.²⁶

Hardware Sandboxing. With systems in place to reduce the effectiveness of drone jamming (sandboxing), novel kinetic kill methods will have to be developed.²⁷

Prevention Against Jamming (JAM-ME) Techniques. Jamming is now being leveraged for drone missions into completion.²⁸

Cognitive Avoidance in 4th Generation GPS. GPS systems are becoming increasingly more interference-proof. Long Term Evolution or LTE may soon be used to operate drones at theoretically unlimited ranges without RF links, i.e., cellular base stations will provide theoretically unlimited range.²⁹

New flight modes that have been introduced in UAVs or drones which include obstacle avoidance using ultrasonic sensors, terrain mapping cameras integrated as SoC, follow me, tapfly, active track and sports mode. Better battery systems have been incorporated giving the drone larger

endurance (5230 mAh battery on board the DJI Phantom 4).

CONCLUSION

Endless possibilities exist in designing a system to counter drones which may extend later to UAVs as well as collaborative swarms. A committee needs to be formulated at the apex level which has stakeholders from the defence forces in addition to judiciary, the academia, and industry (to include Defence Public Sector Undertakings).

The anti-drone systems will definitely be expensive owing to the technology involved. However, costs involved should not thwart the innovations. Better rules and regulations need to be formulated to regulate the Unmanned Traffic Management (UTM). A future roadmap has already been laid out for CAR 2.0.30 There is nothing that stops India from finally having a drone vs drone 'dogfight' or a swarm-against-swarm type of architecture. A situation where drones are "scrambled" to engage and nullify a threat will no longer be mere material for fiction. Indeed, drones being used as a 'loyal wingman' are already under test. Systems like HyperTechTraxerTM (UK registered firm, based in Finland) which use nonlethal weapons as well as swarms to monitor sensitive installations have also been made available in the world market.

The strategy to defend space must be based on adapting to the need of the specific environment where the deployment of the counter-drone system is intended. Integration of various sensors and finally redundancy for sensors in number is also imperative. There is a definite need to align the timeframe taxonomy with the prevailing

threat at all levels. Disruptive techniques that have been brought out in this brief will also pave the way for future research and development of whole some systems to thwart adversarial designs. ©RF

ABOUT THE AUTHOR

Lt Col Vivek Gopal is an Instructor at a premier training institute.

ENDNOTES

- Shi, Xiufang, Chaoqun Yang, Weige Xie, Chao Liang, Zhiguo Shi, and Jiming Chen. 2018. "Anti-Drone System With Multiple Surveillance Technologies: Architecture, Implementation, And Challenges".IEEE Communications Magazine 56(4):68-74.doi:10.1109/mcom.2018.1700430. (National Academies of Sciences, Engineering, and Medicine. 2018. Aeronautics 2050: Proceedings of a Workshop In Brief. 2018)
- 2 Haviv, Haim. 2019. "Drone Threat And CUAS Technology: White Paper."
- 3 "Counter Unmanned Aircraft System (CUAS) Capability For Battalion And Below Operations: Abbreviated Version Of A Restricted Report". 2020. National Academy of Sciences. Accessed March 18.
- Shi, Xiufang, Chaoqun Yang, Weige Xie, Chao Liang, Zhiguo Shi, and Jiming Chen. 2018. "Anti-Drone System With Multiple Surveillance Technologies: Architecture, Implementation, And Challenges". IEEE Communications Magazine 56 (4): 68. doi:10.1109/mcom.2018.1700430.
- Rzewuski, S, K Kulpa, P Kopyt, B Salski, K Borowiec, and M Malanowski. 2018. "Drone RCS Estimation Using Simple Experimental Measurement In The WIFI Bands 2018, 695-698". In 22Nd International Microwave And Radar Conference (MIKON).
- Sacco, Giulia, Erika Pittella, Stefano Pisa and Emanuele Piuzzi. "A MISO Radar System for Drone Localization." 2018 5th IEEE International Workshop on Metrology for AeroSpace (MetroAeroSpace) (2018): 549-553.
- Alnuaim, Tareq, Mubashir Alam and Abdulrazaq Aldowesh. "Low-Cost Implementation of a Multiple-Input Multiple-Output Radar Prototype for Drone Detection." 2019 International Symposium ELMAR (2019): 183-186.
- J. Ochodnický, Z. Matousek, M. Babjak and J. Kurty, "Drone detection by Ku-band battlefield radar," 2017 International Conference on Military Technologies (ICMT), Brno, 2017, pp. 613-616, doi: 10.1109/MILTECHS.2017.7988830.
- 9 J. Drozdowicz et al., "35 GHz FMCW drone detection system," 2016 17th International Radar Symposium (IRS), Krakow, 2016, pp. 1-4, doi: 10.1109/IRS.2016.7497351.
- 10 Chang, Xianyu & Yang, Chaoqun & Wu, Junfeng & Shi, Xiufang & Shi, Zhiguo. (2018). A Surveillance System for Drone Localization and Tracking Using Acoustic Arrays. 10.1109/SAM.2018.8448409.
- 11 C. Yang, Z. Wu, X. Chang, X. Shi, J. Wo and Z. Shi, "DOA Estimation Using Amateur Drones Harmonic Acoustic Signals," 2018 IEEE 10th Sensor Array and Multichannel Signal Processing Workshop (SAM), Sheffield, 2018, pp. 587-591, doi: 10.1109/SAM.2018.8448797.
- Z. Zhang, Y. Cao, M. Ding, L. Zhuang and W. Yao, "An intruder detection algorithm for vision based sense and avoid system," 2016 International Conference on Unmanned Aircraft Systems (ICUAS), Arlington, VA, 2016, pp. 550-556, doi: 10.1109/ICUAS.2016.7502521.
- 13 Ganti, Sai Ram and Yoohwan Kim. "Implementation of detection and tracking mechanism

- for small UAS." 2016 International Conference on Unmanned Aircraft Systems (ICUAS) (2016): 1254-1260.
- T. Sosnowski, G. Bieszczad, H. Madura and M. Kastek, "Thermovision system for flying objects detection," 2018 Baltic URSI Symposium (URSI), Poznan, 2018, pp. 141-144, doi: 10.23919/URSI.2018.8406757.
- 15 K. Lee et al., "Identification of a flying multi-rotor platform by high resolution ISAR through an experimental analysis," International Conference on Radar Systems (Radar 2017), Belfast, 2017, pp. 1-5, doi: 10.1049/cp.2017.0435.
- M. A. Govoni, "Micro-Doppler signal decomposition of small commercial drones," 2017 IEEE Radar Conference (RadarConf), Seattle, WA, 2017, pp. 0425-0429, doi: 10.1109/RADAR.2017.7944240.
- P. Zhang, L. Yang, G. Chen and G. Li, "Classification of drones based on micro-Doppler signatures with dual-band radar sensors," 2017 Progress in Electromagnetics Research Symposium Fall (PIERS FALL), Singapore, 2017, pp. 638-643, doi: 10.1109/PIERS-FALL.2017.8293214.
- 18 L3 Technologies. "Countering the drone threat to commercial airports" accessed at https://www.l3-droneguardian.com/white-papers/L3_Technologies_Whitepaper-Countering_Drones_at_Commercial_Airports.pdf
- 19 Krishna Kumar Karothiya, Abhishek Yadav, Abhyuday Mishra, Ankush, Anshul Gupta, Anshul Katiyar, DRONE CATCHER GUN, GLOBAL JOURNAL FOR RESEARCH ANALYSIS: VOLUME-7, ISSUE-2, FEBRUARY-2018.
- T. Multerer et al., "Low-cost jamming system against small drones using a 3D MIMO radar based tracking," 2017 European Radar Conference (EURAD), Nuremberg, 2017, pp. 299-302, doi: 10.23919/EURAD.2017.8249206.
- 21 "Counter-Drone Systems". 2020. Dronecenter.Bard.Edu. https://dronecenter.bard.edu/projects/counter-drone-systems-project/.
- 22 Butterworth-Hayes, Philip. 2018. "Unmanned Airspace: The Latest Counter-UAS Industry Directory Free Download". Unmanned Airspace. https://www.unmannedairspace.info/counter-uas-industry-directory/.
- 23 2020. https://epaper.hindustantimes.com/%20Home/MSharearticle?OrgId=%203250a44d.
- N. M. Rodday, R. d. O. Schmidt and A. Pras, "Exploring security vulnerabilities of unmanned aerial vehicles," NOMS 2016 2016 IEEE/IFIP Network Operations and Management Symposium, Istanbul, 2016, pp. 993-994, doi: 10.1109/NOMS.2016.7502939.
- N. Dalal and B. Triggs, "Histograms of oriented gradients for human detection," 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05), San Diego, CA, USA, 2005, pp. 886-893 vol. 1, doi: 10.1109/CVPR.2005.177.
- 26 Chang, Yunseok. "A Drone IFF and Tracking Algorithm with the Relay Drone and the Beacon System." (2019).

- J. Mead, C. Bobda and T. J. Whitaker, "Defeating drone jamming with hardware sandboxing," 2016 IEEE Asian Hardware-Oriented Security and Trust (AsianHOST), Yilan, 2016, pp. 1-6, doi: 10.1109/AsianHOST.2016.7835557.
- 28 R. Di Pietro, G. Oligeri and P. Tedeschi, "JAM-ME: Exploiting Jamming to Accomplish Drone Mission," 2019 IEEE Conference on Communications and Network Security (CNS), Washington DC, DC, USA, 2019, pp. 1-9, doi: 10.1109/CNS.2019.8802717.
- B. Kelley, G. De La Torre Parra and D. Akopian, "Cognitive interference avoidance in 4th generation GPS," 2015 10th System of Systems Engineering Conference (SoSE), San Antonio, TX, 2015, pp. 410-415, doi: 10.1109/SYSOSE.2015.7151973.
- 30 "DRONE INNOVATION 2019 & CONTEMPORARY CHALLENGES". 2019. Bprd.Nic.In. https://bprd.nic.in/WriteReadData/userfiles/file/201907010629477222182ReportonDrone Innovation2019andContemporaryChallenges.pdf.

Developing an Effective Anti-Drone System for India's Armed Forces



Ideas • Forums • Leadership • Impact

20, Rouse Avenue Institutional Area, New Delhi - 110 002, INDIA Ph.: +91-11-35332000. Fax: +91-11-35332005. E-mail: contactus@orfonline.org

Website: www.orfonline.org