NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

CSDF
Volume: 1, Issue: 1 July 2022
E-ISSN: In Process

Conceptual Model of Counter-drone System to Overcome the Current Underlying Technology Limitations

Naveen Kumar Chaudhary
National Forensic Sciences University, Gandhinagar, India
Email: naveen.chaudhary@nfsu.ac.in

Abstract - Counter-drone technology comprises of a system that is capable of detecting and intercepting drone. A large number of incidents pertaining to use of drones for illegal and criminal purposes have come to light. Drones are available commercially-off-the-shelf (COTS) and criminals are using it to deliver weapons and contrabands. The sophisticated drones are equipped with latest stealth and evade technologies that have further raised new concerns for the security forces and Law Enforcing Agencies (LEAs). In order to check drone related security and unlawful activities, there is a need to place suitable Counter-drone technology. This article reviews the existing Counter-drone underlying technologies, associated legal and regulatory issues, and proposes a conceptual model of Counter-drone system that takes into account the improvements required in the existing design.

Keywords: Drone, Counter-drone system, sensors, detection, interdiction, spectrum, friend or foe

I. INTRODUCTION

The growth of drone technology due to recent developments in sensor technologies, embedded systems, nanotechnologies, navigational systems and on-board processing has boosted the drone market with affordable drones [1]. The latest drones are developed in many shapes and sizes with advanced navigation, surveillance and payload carriage capacity. The growing drone sophistication has led its way into war zones across the globe. There have been large numbers of incidents wherein drones have been used in a military conflict zones. The growing use of drones for military operations in Syria and Iraq is an indication that future war zones will have one additional layer of aerial platform in the arena. This additional layer dominated by sophisticated drones laced with advanced stealth and evasion technologies will pose a new set of challenges for tacticians and strategists. Drone being aerial platform with navigation and payload carriage capacity provides advantage of height that makes its highly desirable for military and security operations. The growth and development in Cyber Physical Engineered systems has further refined the drone capabilities and drone-manufacturing industries have received a major boost. These days highly sophisticated drones are available commercially-off-the-shelf. E-Commerce websites are also selling drones that are highly customisable and it can be used for multiple purposes. This also provides an easy access of sophisticated drones to criminals, terrorists, insurgents and anti-social elements. A large number of incidents have come to light wherein drones have been used in criminal activities [2-5]. ISIS has trained and skilled its terrorists to assemble drone and fabricate drone guided IEDs towards target with precision. They have launched successful attack against the specified targets with explosive laden drones [6]. The use of drones by ISIS, Hezbollah, Houthis and militant groups in Ukraine has added a new dimension to terrorism. The non-state actors and terrorist groups are using drones against their targets by taking the advantage of mountains, inhospitable terrain and area of thick foliage coupled with the porous borders of a pliant state [7]. The drone related incidents are on the rise as handlers find it easy to operate the drone remotely and accomplish the illegal activities covertly. In September 2018, an incident wherein rouge drone was involved in dropping arms and satellite phone in the border state of India came to light [8]. A rogue drone was also sighted and shot-down in the northern border state of India in June 2020, the customised drone was carrying arms and ammunition [9]. A few incidents have also come to light wherein adversary's drone after dropping the payload successfully returned to its handlers evading the detection. The drone related criminal and cross-border illegal activities can be checked effectively by placing suitable Counter-drone mechanism.

II. COUNTER-DRONE TECHNOLOGY

The Counter-drone technology is also known as Counter-Unmanned Aerial Vehicle (UAV) technology. UAV is an aircraft without a human pilot on board and it is a part of Unmanned Aircraft System (UAS), which includes a UAV, a ground based controller and a system of communication between the two [10]. The word Drone and UAV means the same thing, and can be used interchangeably. The Counter-drone industry has grown exponentially in the recent years and many products are available across the globe. The growth in Counter-drone technology can be largely attributed to the rising use of drones by the adversaries, terrorists and criminals. A few terrorist groups like ISIS have demonstrated advanced skillset in operating wide range of drones and its customisation. In the recent years, the drone related crimes in India have also increased and many violations of DGCA regulations have come to light amid COVID-19 pandemic. A

few cases of close encounters between drones and manned aircraft have been also reported in the Indian airspace. A rogue drone which violated Indian air space along the international border in Anupgarh, Rajasthan in February, 2019 was shot down by the fighter jets [11]. The possible threat of using drone as a weapon against a large crowd and vital installations has given a new momentum to Counter-drone industry. The Counter-drone system contains various types of sensors for detection and interdiction [12-13]. The statistics of various interdiction and detection systems available globally as of 2019, is shown in figure 1, [12]. The generic block diagram of the Counter-drone system is shown in figure 2.

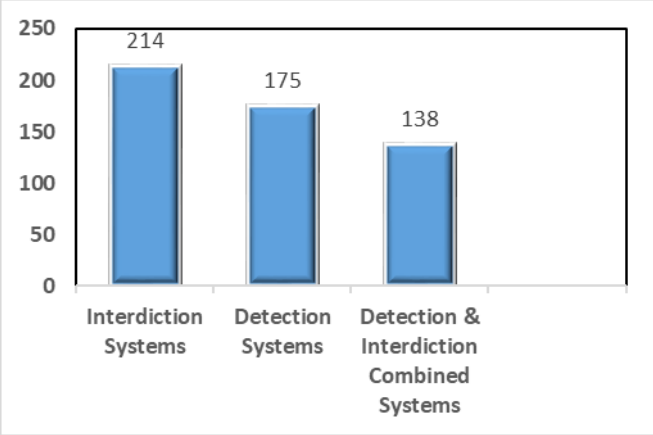

Fig. 1. Counter Drone systems statistics.

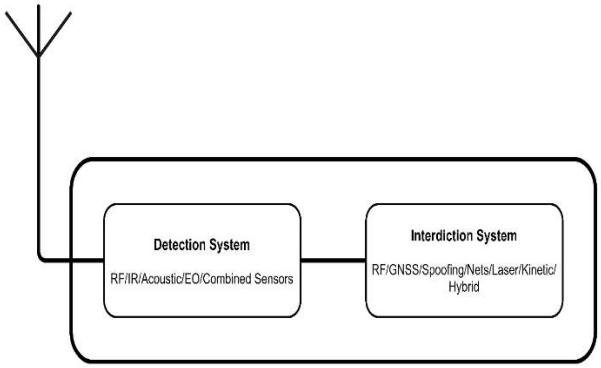

Fig. 2. Generic Counter-drone system block diagram.

III. Counter Drone Detection Technologies

Radio Frequency (RF), Electro-Optical (EO) and Infra-Red (IR) based drone detection systems are quite popular. While jamming, is a most popular interdiction technique. The underlying detection and interdiction technology also pose a wide range of legal, regulatory and practical issues. The Counter-drone systems available commercially are ground, hand-held and Drone platform based. The ground-based systems can be used from stationary as well as mobile positions on the ground. The hand-held systems are designed to be operated by a single user. Drone-based systems are designed to mount the interdiction system on the drone and target the intended system at a close range. The detection and tracking of the target in a Counter-drone system can be either performed by Radar or different sensors. The Radar detects the drone by its signature. The signature is generated when the Radar emitted RF pulses bounces back after encountering the drone [14]. A specialised algorithm is applied to distinguish between the low-flying objects and actual drone. The Radio Frequency (RF) sensors are also used for drone detection. The RF based drone detection system scans the spectrum in which drone works and it geo-locates the detected device using appropriate algorithm [15]. The Electro-Optical (EO) system detects drone based on their visual signature. The Infra-Red (IR) detects drones based on their heat signature and Acoustic based sensors work by recognising the unique sounds produced by the drone motors. It relies on the libraries of the known drones' acoustics. Many Counter-drone systems use mix of sensors to enhance the drone detection rate and realise a robust detection system [15].

IV. Counter Drone Interdiction Technology

Radio Frequency Jamming is the most popular interdiction technique. In this technique, the link between the drone and its operator is disrupted by generating large volume of RF output. On being jammed the drone either descends to ground or initiates return to home manoeuvre. The other popular interdiction technique is 'GNSS Jamming'. In this technique, the Global Navigation Satellite System (GNSS) link which is used for the navigation of drone is disrupted. The drone on disruption of GNSS link either hovers in air, lands on ground or initiates return to home manoeuvre. Spoofing or 'Protocol Manipulation' is also one of the interdiction techniques but it is not a very popular technique due to its complexity and effectiveness. In this technique the control of the drone is taken over by targeting the drone's communication link.

There is also a rise in the Laser based interdiction techniques wherein Laser energy is directed towards the targeted drone's airframe that burns or crash the drone to the ground. A kinetic method is also used for drone interdiction. A net is thrown towards the targeted drone through a projectile in the air to entangle the drone or its rotors. An ammunition based projectile systems are also used to destroy the targeted drone in the air. A few manufacturers are also developing drones which can chase and engage rogue drones in the air as a part of their Counter-drone system. In order to achieve robustness in interdiction, Counter-drone systems employ combination of interdiction techniques. RF cum GNSS jamming is the most common interdiction technique. Figure 3, shows the statistics of different interdiction sensors as of 2019 that have been used in Counter-drone systems [12].

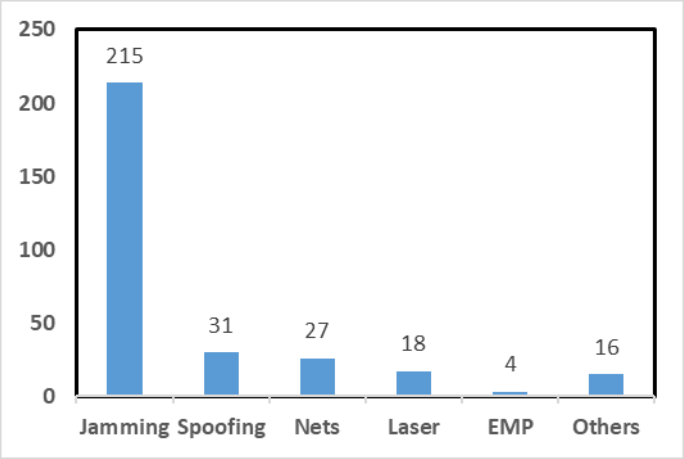

Fig. 3. Statistics of different interdiction sensors used in Counter drone systems.

V. Limitations of Counter-drone Technology

The effectiveness of the Counter-drone system is based on many factors, however no system can claim to be hundred per cent effective as every detection and interdiction technique has some drawbacks. The Radar systems at times fail to detect drones as majority of the commercial drones fly at relatively low altitude and their Doppler signatures are small. EO system only works during the day when visibility is good. In order to have day as well as night detection capabilities, Counter-drone system incorporates two or more sensors like EO as well as IR. The majority of RF based detection systems work well within line-of-sight and suffers degradation when the link is lost or signal fades. The acoustic based sensors works well when the acoustic signatures are updated and available in the library. It will turn deaf to drones not covered by the acoustic library. It's really challenging to keep the library updated considering the rate of proliferation of new commercial drones in the market. The country specific spectrum regulations and laws regarding interception have bearing on the sensors operation besides its own technical limitations. The limitations of sensors and emitters are shown in table 1 and table 2, respectively.

Table 1: Limitations of sensors.

Sensors	Limitations
RF	Bad weather.
EO	Bad light and visibility
IR	Works in night
Acoustic	Works only if signature is available in the library.
Combined Sensors	Enhances detection capability but adds to cost and complexity.

Table 2. Limitations of emitters used in interdiction of drones.

Emitters	Limitations
RF Jamming	Legal implications.
GNSS Jamming	Legal implications and difficult to implement in multi-GNSS systems.
Spoofing	Legal implications and effective against only vulnerable drones.
EMP	Legal implications and hazardous for operating environment.
Laser	Legal implications and hazardous for operating environment in case it deviates from the target.

A. Identification of Friend or Foe

A large number of drones are employed these days for surveillance purposes. The drones are very effective for intelligence, surveillance and reconnaissance purposes [16]. Drones are very useful when it comes to monitor any area through an aerial view or cover any major sporting, cultural or political event. In a large sporting, political or cultural event many legitimate drones are employed for cinematography and surveillance purposes. In such events, an intrusion by single rogue drone with malicious intent may pose serious security risk, however there is a no full-proof Counter-drone solution available commercially which can identify whether the drone is legitimate or rogue (friend or foe). The rogue drones are being viewed as a big threat to stadiums and open-air events [17]. Counter-drone system with capability to identify friend or foe drone is required to tackle the threat of rogue drones.

B. Counter-drone System Standardization, Legal and Regulatory Issues

The design, make and technology of Counter-drone system varies from one manufacturer to another. There is no globally recognized standard for Counter-drone system design and use. This variation raises safety, design and reliability related issues in the Counter-drone systems. The interdiction techniques used in the Counter-drone system either uses jamming or directed energy. This also poses regulatory and legal challenges as both of these interdiction techniques may fall under the category of unlawful activity in many countries. Besides that, the spectrum allocation and monitoring are governed by the respective laws and regulations of the country. The spectrum regulatory norms may also vary from one country to another; therefore, the frequency of the interdiction system, if not harmonized properly may cause

serious interference in the operating environment and disrupt operational communication links in the vicinity.

C. Hazards Associated with Kinetic Counter-drone Systems

The drones that are targeted by physical means at times pose serious risks. The projectile or ammunition based kinetic systems on targeting the drone make it fall abruptly on the ground. Even the net-based systems with parachute mechanism intended to bring the entangled drone on the ground may turn risky. In both of these cases the drone loses its control on being targeted by the physical means and it may go haywire before hitting the ground.

VI. PROPOSED COUNTER-DRONE MODEL

The Counter-drone system comprises of monitoring, classification, location, tracking, alerting and Counter-drone modules. Drone monitoring equipment can be passive or active. The passive system remains on listening mode wherein active system emits signal and analyses what comes back. The detection module encompasses the technology that detects the drones. It is important to detect whether the aerial platform is actually a drone, or any other flying object. The locating and tracking module helps in situational awareness of the drone. The alerting module sends trigger to deploy the countermeasure. The countermeasure techniques can be technology or non-technology based solution. Radio Frequency Jammers, GPS Spoofers, High Power Microwave devices, High Energy Lasers and Net Guns are technology driven solutions. Training and employing highflying birds to intercept drones that is also known as 'Birds of Prey' is a non-technical solution. The building blocks of the generic Counter-drone system are shown in figure 4.

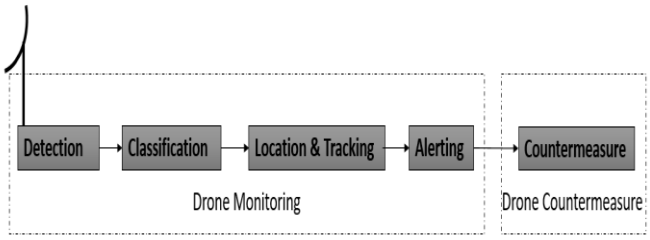

Fig. 4. Counter-drone system building blocks.

The proposed model contains two additional building blocks these are 'Spectrum Compliance' module and 'Friend and Foe' Identification module. The 'Spectrum Compliance' module assumes greater significance when active monitoring technique is used in the Counter-drone system. The active system emanates the signal and the frequency of the emission depends on the nature of emitter that is used. In order to ensure that active system emits the signal within the prescribed regulatory spectrum of the country, the 'Spectrum Compliance' module has been proposed. This module will scan the emitted frequency and block the emission if it violates the prescribed regulatory spectrum limits. This will assist in maintaining the overall spectrum harmony and avoid the RF interference even if the Counter-drone system has to be operationalised in the nearby vicinity of airport and wireless monitoring and broadcasting stations. The 'Spectrum Compliance' module should contain the table with the predefined spectrum limits for each emitter as per the prescribed spectrum regulation and monitor the frequency for any violation. In case of violation, it should block the frequency to the prescribed limit. The second proposed module is 'Identify Friend or Foe'. The countermeasure techniques need to be used only if the drone is rogue or hostile. The unfriendly drones need not be intercepted and engaged. A mechanism to identify whether the drone is friendly or foe will resolve this issue. Many countries across the globe have adopted regulations on drone and that makes registration of new drones mandatory with the regulatory authority. The regulatory authorities should adopt a mechanism of registering drone's MAC address and that should be shared with the registered Counter-drone manufacturers with a provision to update the database periodically so the MAC address of the newly registered drones are updated in manufacturers' database as and when new drones are registered. The proposed model with two additional building blocks are shown in figure 5. The model with additional modules has been proposed to do away the shortcomings in the design of Counter-drone architecture.

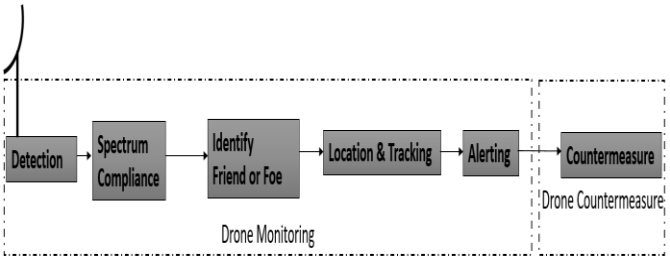

Fig. 5. Proposed Counter-drone model with two additional building blocks.

A. Spectrum Compliance Module

The 'Spectrum Compliance' module will primarily provide a frequency monitoring mechanism. It will contain the upper and lower prescribed frequency limits of each emitter as per country's spectrum regulation. The spectrum database repository will contain the emitter frequency details. The frequency band limiter will ensure that operating emitter remains in the prescribed frequency band. The conceptual model of the spectrum compliance module is shown in figure 6.

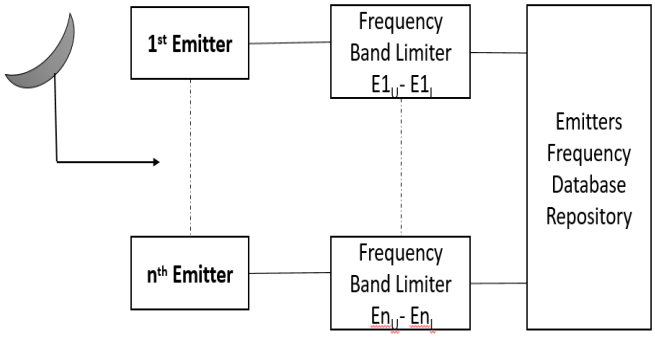

Fig. 6. Conceptual model of Spectrum Compliance.
$E1_U$: First Emitter predefined frequency upper band.
$E1_L$: First Emitter predefined frequency lower band.
En_U: nth Emitter predefined frequency upper band.
En_L: nth Emitter predefined frequency lower band.

B. Identify Friend or Foe Module

The concept of identify 'Identify Friend or Foe' module is based on a portable WiFi receiver capable of detecting Wi-Fi signature of the on-the-fly drone. The WiFi enabled drone emits signal that can be captured and discerned. The signal contains a unique identifier, called the MAC identifier of the drone. MAC is a 6-byte globally unique identifier. The first three bytes of this address indicates organisationally Unique Identifier (OUE) that is bought by vendors from IEEE registration authority. The last three bytes are the Network Interface Controller (NIC). The WiFi range extender may be used as a contraption to detect on-the-fly drone from the distance. The receiver on detection of the drone should identify the MAC number of the drone and compare the same with the available MAC database repository. If the MAC address of the on-the-fly drone matches with the record available in the repository, it will flag it as a friendly drone. If the MAC address of the on-the-fly drone does not match with the records available in the database, it will flag the drone as a foe and decision to engage the drone through suitable countermeasure techniques can be taken. The conceptual block diagram of identify 'Identify Friend or Foe' module is shown in figure 7.

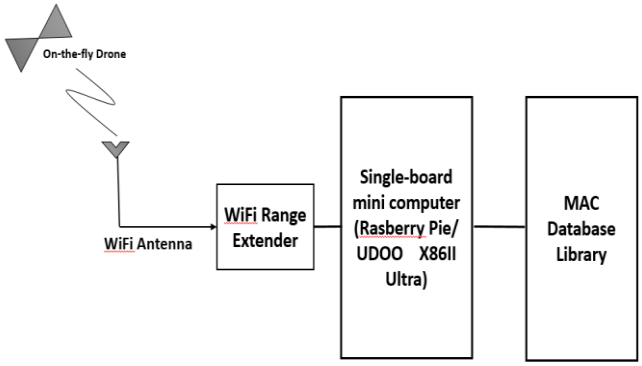

Fig. 7. Conceptual model of identify friend or foe module.

VII. CONCLUSION

The Counter-drone technology has become an indispensable requirement for law enforcement agencies and security forces. The Counter-drone technology is evolving and it needs to be in compliance with the new regulatory norms that has been introduced by many countries to counter drone related security threats. The Counter-drone system needs to operate in harmony with spectrum regulation and legal obligations of the state. The paper reviewed the Counter-drone system underlying technologies and identified the areas where improvements are required to make it suitable for use as per the legal and regulatory requirements. A conceptual model of two modules; 'Spectrum Compliance' and 'Identify Friend or Foe' has been proposed for incorporation in the existing Counter-drone system design. The former module conceptually caters for all types of emitter that may be used actively in the Counter-drone system for tracking on-the-fly drone, however the latter module only caters for the drones that are controlled through the WiFi signal. With the evolution of Cyber Physical Engineered System and mobile cellular communication, the use of cellular technology to control the drone is also gaining the momentum. The complexity of the drone controlling mechanism will grow further with the adoption of 5G technology. This entails expansion of 'Identify Friend or Foe' module with evolving technologies as a future work.

REFERENCES

[1] F Kamoun , H Bouafif H and Iqbal F, "Towards a Better Understanding of Drone Forensics: A Case Study of Parrot AR Drone 2.0," International Journal of Digital Crime and Forensics, vol. 12, issue 1, Jan-Mar 2020.
[2] A. P. Cracknell, "UAVs: Regulations and Law Enforcement," International Journal of Remote Sensing. vol. 38, no.8-10, 2017, pp.3054-3067.
[3] T. M. Ravich, "Courts in the Drone Age. Northern Kentucky Law Review," vol.42, no.2, 2015, p.161.
[4] L. E. Buckley, "Recreational UAVs: Going Rogue with Pennsylvania's Strict Products Liability Law Post Tincher," University of Pittsburgh Journal of Technology Law & Policy, vol.15, 2014, p.243.
[5] S. Maddox and D. Stuckenberg, "Drones in the U.S. National Airspace System: A safety and security assessment,'" Harvard Law School National Security Journal, Feb, 2015. Available: https://harvardnsj.org/2015/02/drones-in-the-u-s-national-airspace-system-a-safety-and-security-assessment/(Accessed Sept. 3, 2021).
[6] Susannah George and Lori Hinnant, ISIS Using Drones, Other Innovating Tactics with Deadly Effect. The Associated Press, 2017.
[7] Lt Gen R S Panag (Retd.), "Beyond sea and land, India's next defence challenge is drone terrorism", The Print, Feb. 7, 2019. [Online], Available: https://theprint.in/ opinion/beyond-

sea-and-land-indias-next-defence-challenge-is-drone-terrorism/188749/(Accessed Sept. 4, 2021).
[8] Manjeet Sehgal, "8 days, 10 sorties: Pakistan drones dropped AK-47 rifles, 80kg ammunition in Punjab", India Today, Sep 25, 2019. [Online], Available: https://www.indiatoday.in/indi/story/pakistan-drones-ak47-rifles-ammunition-tarn-taran-1602906-2019-09-25 (Accessed Sept. 5, 2020.
[9] Ravi Krishnan Khajuria, "Arms-laden Pak drone shot down by BSF along International Border in J&K's Kathua", Hindustan Times news, June 20, 2020. [Online], Available: https://www.hindustantime.com/india-news/pakistani-drone-shot-down-by-bsf-along international-border-in-jammu-and-kashmir-s-kathua (Accessed Sep. 5, 2020.
[10] Lous de Gouyon Matiynon, "Drones: New Uses, New Regulations, New technologies," May, 2019, Available: https://www.spacelegalissues.com/drones-new-uses-new-regulations-new-technologies (Accessed Sept. 6, 2020).
[11] Snehesh Alex Philips, "Pakistani drone violates Indian air space along international border, shot down by IAF", The Print, Mar. 4, 2019. [Online], Available: https://theprint.in/defence/ Pakistanidrone-violates-indian-air-space-along-international-border-shot-down-by-iaf/201207/, (Accessed Sept. 6, 2020).
[12] Arthur Holland Michel, "Counter-drone systems. Dec 2019," 2nd edition, project report. Available: https:// dronecenter.bard.edu/files/2019/12/CSD-CUAS-2nd-Edition-Web.pdf, (Accessed Oct. 7, 2020.
[13] Unmanned Aircraft System Detection -Technical Considerations," U.S. Federal Aviation Administration, 2019, Available:https://www.faa.gov/airports/airport_safety/media/ Attachment -3-UAS-Detection-Technical-Considerations.pdf, (Accessed Oct. 7, 2020).
[14] F. Hoffmann, et al., "Micro-doppler based detection and tracking of UAVs with multistatic radar'" Proc. IEEE RadarConf, Philadelphia, PA, USA, May 2016, pp. 1–6.
[15] X. Shi, C. Yang, W. Xie, C. Liang, Z. Shi and J. Chen, "Anti-Drone System with Multiple Surveillance Technologies: Architecture, Implementation, and Challenges." *IEEE Communications Magazine*, vol. 56, no. 4, Apr., pp. 68-74, 2018.
[16] Dr. Monika Chansoria, "Proliferated Drones: A Perspective on India," Available: http://drones.cnas.org /wpcontent/uploads/2016/06/A-Perspective-on-India-Proliferated-Drones.pdf, (Accessed Oct 9, 2020.
[17] Atul Pant, "Drones: An Emerging Terror Tool," Journal of Defence Studies. Vol. 12, No. 1, Jan-Mar 2018, pp. 61-75, 2018.