Investigating Cost-effective RF-based Detection of Drones

Phuc Nguyen[†], Mahesh Ravindranathan[‡], Anh Nguyen[†], Richard Han[‡] and Tam Vu[†]
[†]University of Colorado, Denver, [‡]University of Colorado, Boulder
{phuc.v.nguyen, anh.t4.nguyen, tam.vu}@ucdenver.edu,
{mahesh.ravindranathan, richard.han}@colorado.edu

ABSTRACT

Beyond their benign uses, civilian drones have increasingly been used in problematic ways that have stirred concern from the public and authorities. While many anti-drone systems have been proposed to take them down, such systems often rely on a fundamental assumption that the presence of the drone has already been detected and is known to the defender. However, there is a lack of an automated cost-effective drone detection system. In this paper, we investigate a drone detection system that is designed to autonomously detect and characterize drones using radio frequency wireless signals. In particular, two technical approaches are proposed. The first approach is active tracking where the system sends a radio signal and then listens for its reflected component. The second approach is passive listening where it receives, extracts, and then analyzes observed wireless signal. We perform a set of preliminary experiments to explore the feasibility of the approaches using WARP and USRP software-defined platforms. Our preliminary results illustrate the feasibility of the proposed system and identify the challenges for future research.

Keywords

UAVs, Drone Detection; Wireless Technology; RF.

1. INTRODUCTION

The development of inexpensive embedded sensors and miniaturized electronics enables the rapid proliferation of new civilian uses of unmanned aerial vehicles (UAVs) or drones. As its cost falls, owning a drone is easier than ever before. Drones are being used for a wide variety of applications, including aerial photography and video, mapping/ surveying, search and rescue, precision agriculture, and scientific research [20]. Amazon has proposed to employ drones in the future for airborne delivery of packages (Amazon Prime Air) [11].

Beyond their benign uses, civilian drones have increasingly been used in problematic ways that have stirred concern from the public and authorities. For example, on March 29, 2016, a Lufthansa jet came within 200 feet of colliding with a drone near Los Angeles International Airport (LAX) [30]. Drones have also interfered with fire-fighting aircraft being used in the region of forest fires [22]. A drone crash interrupted a U.S. Open tennis match [33], prompting one of the players to say “It was a little bit scary, I have to say, because with all the things happening now in the world, I imagine maybe it’s a bomb." Another drone crashed at the White House, raising concerns about security risks to government buildings and facilities [18]. In addition, drones have been accused of being used to stalk people and violate their privacy [23].

Many anti-drone systems have been proposed to disable the flight capability of drones and thereby combat the threats posed by such drones. One approach is to shoot a net at the flying drones to physically bring them down and prevent further flight [29]. Another approach is shoot a laser beam at the drone to disable it [32]. Another solution has been proposed to deceive the drone’s localization system by spoofing GPS [17]. A further approach is to use electronic means to gain control over these drones, hacking into the drone and hijacking its controller by issuing control messages to the approaching drone [27]. Of course, the simplest approach has been to shoot down a drone [7]. A fundamental assumption of all of these approaches is that the presence of the drone has already been detected and is known to the defender. While there have been a few systems proposed to detect drone’s presence (see Sec. 5), automated cost-effective drone detection systems are lacking both in the literature and in industry.

In this work, we propose to investigate the use of inexpensive commercial off-the-shelf (COTS) technology, e.g. WiFi and inexpensive software-defined radios (SDR), to automatically detect drones. We present two main methods, *active* to detect the drone by observing the reflected wireless signal, and *passive* to listen to the communication between the

DroNet’16, June 26 2016, Singapore, Singapore

DOI: http://dx.doi.org/10.1145/2935620.2935632

drone and its controller. The system includes a receiving antenna and a transmitting antenna. In the active approach, the transmitter continuously broadcasts out wireless signal. The receiving antenna then listens to and captures the reflected signal which bounces off the drone. This reflected signal, which may contain a unique signature caused by the drone, is then analyzed to conclude about the presence of the drone and its physical characteristics. In the *passive* approach, only the receiver is needed to detect the drone by listening to and analyzing the communication signal created by the drone and its remote controller.

Our work makes the following contributions: we first discuss the possible solution and challenges of inexpensive autonomous RF-based detection of drones; we further present early feasibility experiments demonstrating some of the challenges and opportunities of cost-effective RF detection.

The following section discusses our system assumptions and a variety of challenges that we face. We then discuss our drone detection principle. Next, we describe a variety of RF measurements that we have taken with drones to explore the challenges enumerated previously. We conclude the paper with a discussion.

2. CHALLENGES AND SYSTEM ASSUMPTIONS

We begin by making certain assumptions about the drone detection and target systems. First, we assume that our detection system should consist of low cost COTS components, such as WiFi access points and inexpensive SDRs, e.g. the Ettus B200 costs less than $1K. Second, in terms of the target drones, we assume that they are commercially available such as DJI [15], Parrot [24], and hobbyist drones. These drones are typically equipped with a number of propellers, and wirelessly controlled by a remote controller that operates on typical unlicensed radio frequency bands such as 2.4Ghz or 5.1Ghz. Moreover, the drone also emanates a radio frequency signal to communicate back to its remote controller for controlling and status signals (e.g. battery level, wind level, balance, acknowledgment) or for transferring data (e.g video recorded, location, etc).

Given these assumptions, the key challenges in developing an RF-based drone detection system include:

- Range: Since the signal drops quickly over distance, the system needs to pickup the signal with high sensitivity.
- Noise: Since the RF band is unlicensed, it is heavily used by others such as Wi-Fi devices. Hence, we need to be able to eliminate noise by identifying prominent features caused uniquely by drones.
- Speed/time: Given the high speed of drones and limited RF detection range, it is important for the system to scan and capture the signal quickly before the drone goes out of range.
- Urban environment: Many of the problematic scenarios involving drones occur in urban environments with buildings around in which RF interference and multipath may be exacerbated. Therefore, the system needs to be designed to address issues caused by multipath effects.
- Low cost: The detection system needs to be constructed from COTS components to maintain a low total cost.

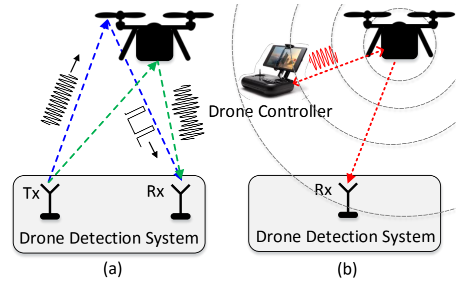

Figure 1: The overview of drone detection system: (a) *active* and (b) *passive* approaches.

We note that while overcoming all of these challenges are critical to realize the proposed system, we now only discuss about the challenges regarding range, noise, and urban environment in this work and aim to addresses the remaining (speed/detection time) in the future. In addition, we will also present the key challenges of realizing proposed solutions.

3. DRONE DETECTION PRINCIPLE

In this section, we present different approaches for drone detection with RF technology. Our proposed solutions rely on three main sources of wireless signals caused by *the drone's rotating propellers*, *the drone's communication* and *drone's body vibration*.

+ Drone detection by analyzing the reflected signal from the drone's propellers. In general, the drone is detected based on the signature of the signal reflected from its propellers, which could be observed by off-the-shelf wireless receiver (i.e Wi-Fi receiver or WARP). This proposed system could be implemented by *active* approach as illustrated in Figure 1(a). Similar to a radar, a transmitter broadcasts and a receiver captures the reflected signals bounced off the drone. The reflected signal is not continuous and its duty cycle depends on the rotation speed and size of the propeller, and the distance between the drone and receiver.

For example, if the propeller rotates with the speed around 7500 to 10500 RPM (as in Bebop ARDrone [19]), we expect to see the signature of the drone on the frequency band less than 200Hz. However, the reflection capability depends on the drone orientation and distance with respect to the wireless receiver. As will be shown in the later experiment (Section 4), the signal is not fully reflected after passing through the drone propellers, we found that there is a significant difference between scenarios with and without the drone within the band of 20^{th} Hz to 30^{th} Hz on the received signal.

+ Drone detection by eavesdropping on the communication between the drone and its controller. Technically, the system detects a drone by listening the communication channel between the drone and its controller using a wireless receiver. The proposed system includes a wireless receiver that listens at the drone's communication frequency range. As mentioned in existing literature [26, 14, 12], most of the drones usually communicate with their controllers frequently around 30 times per second to update its status as well as to receive the commands from controller. Unlike the communication channel between access point (AP) and mobile devices (mobile phone, tablet, and laptops) at home environment, which usually exchang beacons at every 100ms (10Hz) [16], the drone controller requires higher frequency of communication to control the drone precisely. Therefore, a system could collect wireless samples and observes the signal at frequency band less than 100Hz, analyses them, and detects drone's presence. The preliminary validation of this idea is presented in Section 4.

+ Drone detection by analyzing the vibration patterns of the drone's body. This method can be implemented using either *active* or *passive* approach. In *active* approach, the system sends out a wireless signal and observes the reflected component caused by drone body vibration. In *passive* approach, the wireless receiver observes the signal overheard from the drone communication, and analyzes the received signal caused by drone's body vibration. More specifically, the receiver observes the change in reflected signal strength caused by the drone body's vibration. The minute distance changes between the drone and receiver can be estimated on both received signal strength (RSS) or phase variations. Let d be the distance between the drone and controller, Δd be the distance variation caused by the drone's body, then the RSS of the signal can be estimated from the well-known path-loss equation:

$$RSS = \gamma G^2(d + \Delta d), \tag{1}$$

where $0 < \gamma < 1$ is the reflection capability of the drone's body, and the gain G is the attenuation gain of signals due to round-trip propagation. Then, we can approximate the relationship between RSS and distance change. The fluctuation of the RSS represents the change of Δd. The variation patterns then would be used to detect the drone. For better resolution of distance variation detection, we can analyze phase of the received signal. The principle of phase-based analysis is inspired from a traditional equation in wireless technology:

$$\phi = \frac{2\pi \times \text{distance}}{\text{wavelength}} = \frac{2\pi \times (d + \Delta d)}{\lambda}, \tag{2}$$

where ϕ be the phase and λ be the wavelength of the received signal. Then, the variation patterns Δd can be observed and analyzed to detect the drone.

4. EXPERIMENTAL VALIDATION

In this section, we conduct a set of controlled experiments to validate the feasibility of our approaches as well as to describe the related research problems. The experiment setup is shown in Figure 2. In the *active* approach, we place a drone from 0.5m to 5m away from the wireless transmitter and receiver and collect the data when the drone is flying and powered off. In the *passive* approach, a similar setup is used, but the wireless research platform does not emit any signal and only listens the wireless signal in the vicinity. Both drone and wireless research platform are operating on WiFi 802.11 standard (channel 6, 2.437 GHz) during our experiments, and the sampling rate of data collection process is 100kHz.

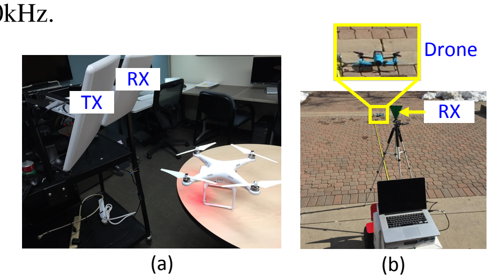

Figure 2: The experiment setup to validate the availability of the drone by using (a) *active* and (b) *passive* approaches.

+ Drone detection by analyzing the signal reflected off of the drone's propellers. We validate the feasibility of the proposed approach by analyzing the reflected signal strength on both time and frequency domains when sending a single tone RF signal to the drone. We used a Wireless Research Platform board (WARP [21]) for this approach (Figure 2(a)).

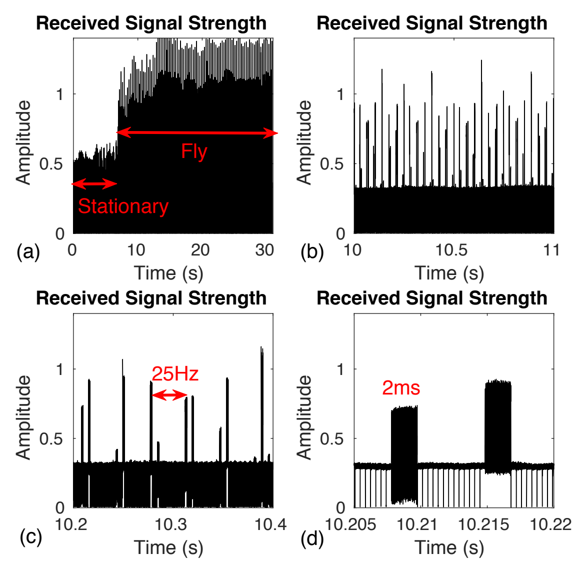

Figure 3: The results of observing the reflected signal using the *active* detection approach.

We plot the received signal strength of the signal captured by the *active* approach as in Figure 3. We display the signal on different time scales when zooming in the signal strength from (a) to (d). As can be seen in Figure 3(a), the received signal strength increases significantly when the drone changes from stationary mode to flying mode (propellers rotating). In Figure 3(c), we observe that the effects of the reflected signal mostly appeared at low frequency components (less than 100Hz). We found that the length of each reflected signal varies from 1.4ms to 2ms. From the above results, it is feasible to observe the reflected signal from a drone's propeller on the time domain, and this signal can be used to develop an algorithm for drone detection. We also found that the difference between stationary and flying stages of the drone in terms of received signal strength (as illustrated in Figure 3) can be observed clearly when the distance between the drone and the detecting system is less than 3m. We are investigating a complete detection algorithm and validating it with longer distance.

Challenges. We found interesting research problems when investigating on this technique: (a) The drone propeller is too small, and the disturbance caused by its rotation is difficult to be observed; (b) The angle of the beam direction and the propellers affects the sensitivity of the detection algorithm; (c) The drone usually flies with 10m/s making it challenging to obtain enough wireless disturbance to deduce the drone availability; (d) The communication between the drone and its controller also creates the effects to the signal at 30th Hz frequency, hence, distinguishing the signal caused by the drone's communication and the propellers rotation is one of the key challenges.

+ Drone detection by eavesdropping on the communication between the drone and its controller. We use USRP Ettus B200 board [28] to validate the feasibility of the approach. The setup is illustrated as in Figure 2 (b). As the drone communicates with its controller frequently around 30 times/s [26, 14, 12], by eavesdropping this communication channel and observing the frequency range from 20Hz to 100Hz, we observe a clear effect from the presence of the drone from the received signal. Figure 4 (top left) shows the frequency distribution of the signal by placing a drone 5m away from the USRP board. As illustrated in the figure with blue-dotted cycles, there are peaks that can be observed at 30th, 60th, and 90th Hz when the drone is flying. Note that there are four main components that might cause those peaks: *the motor rotation*, *the camera feed*, *the propeller rotation*, and *the communication channel*. To confirm that these peaks are from the communication channel, we isolate each of these components and observe the received signal in frequency domain. We found that the drone's signature (30th, 60th, 90th Hz peaks) is occurred regardless of the availability of motor rotation, camera feed and propellers rotation. Table 1 describes the detailed experimental results. As can be seen from the table, the drone signature is only observable when the communication between the drone and its controller is established. The signature is observable even when we disable the camera, stop the motor, and remove the propellers.

We then conduct two further experiments to answer the key questions: *"How far can the drone's signature be observed?"* and *"How does the environment affect to the drone's signature?"*. The following discussion describes the answers in details.

Impact of Distance Change. We setup an experiment as in Figure 2 (b). We vary the distance from 5m to 50m, and observe the signal in time and frequency domains. The RSS drastically reduces when the drone is moved from 5m to 50m away from the receiver. With the presence of the drone, the RSS is higher than the noise level when the distance is less than 50m. The RSS is close to the noise level when the distance between the drone and the receiver is around 50m. Moreover, we plotted the collected signal in the frequency domain as in Figure 4. The signal peaks caused by the communication channel are marked as *signature* peaks at about 30th, 60th and 90th Hz inside the dotted blue cycles. The characteristics of the received signal on frequency domain remain similar over different distances. These results are repeated over 5 testing sessions.

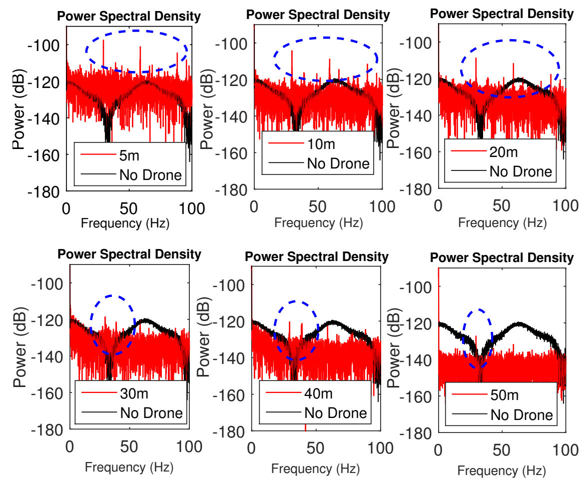

Figure 4: The frequency distribution of the received signals observed at different distance with the drone using the *passive* detection approach.

Drone - Controller Comm.	Motor	Camera Feed	Propeller	Drone Signature
No	Off	Absent	Absent	No
Yes	On	Absent	Absent	Yes
Yes	On	Absent	Present	Yes
Yes	Off	Absent	Absent	Yes
Yes	Off	Absent	Present	Yes
Yes	On	Present	Absent	Yes
Yes	On	Present	Present	Yes
Yes	Off	Present	Absent	Yes
Yes	Off	Present	Present	Yes

Table 1: A summary of experiment setup to validate the signature of Drone's communication.

So far, we have shown that the drone's signature can be observed by eavesdropping on the drone's communication. However, this signature is sensitive to the distance between the drone and the detecting system. It is challenging to observe the drone's signature when the distance is around 50m or more. This limitation, however, can be partial solved by increasing the gain of the receiver's antenna panel. Note that we are currently using an antenna panel that supports very small gain (6dBi).

Next, we answer the second question mentioned earlier. More specifically, we want to validate the possibility of this technique when changing the testing environment.

Impact of Environment Change. To validate the effects of environmental change, we setup an experiment as in Figure 5, where we control the drone to fly in a downtown city (inside our campus) and in an open field (soccer field). In the

Figure 5: The setup to validate the effects of changing the environments: at our campus in a downtown city (a) and at an open field (b).

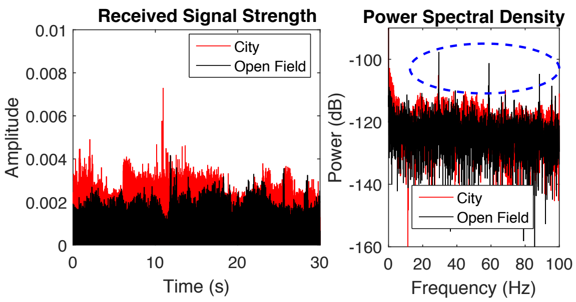

Figure 6: The received signal strength observed in a city and an open field.

city environment, there are many Wi-Fi APs operating at the same frequency of the drone (at least 5 APs have been found at the time and the maximum received signal strength varied from -40dB to -90dB). Meanwhile, there is only one WiFi channel in the open field operating at the drone's frequency with -90dB maximum signal strength. The results are shown in Figure 6. As can be seen from the Figure, the higher received signal strength is obtained in the city environment because the wireless receiver receives data from different sources beside of the drone. More importantly, both received signal maintain the peaks as can be seen in frequency domain (Figure 6 (right)). The results are repeated during 5 testing sessions. Therefore, these results confirm that the presence of the drone can also be observed in a city environment.

In summary, the preliminary results showed that our method is very promising for addressing the drone detection problem. The drone can be detected by its *signature* based on observing the wireless signal in the area that it passes through.

Challenges. We also found interesting research problems when investigating this technique. The current detection mechanism relies on the fact that the drone is required to exchange the information with its controller frequently (30 times/s). This frequency of communication is distinguishable with the frequency of exchanging beacons between mobile or tablet or laptop and home devices with WiFi AP [16]. However, one can develop an application to communicate with an AP at the same frequency as the drone (30Hz). Therefore, we are looking deeper into the obtained WiFi package of the drone to analyze the key differences between the drone's communication packages and others. In addition, regarding the impact of changing the drone's flying speed, we need to do further experiments as it was difficult to obtain the proper flying speed from our drone controller during the testing sessions.

+ Drone detection by analyzing the movement patterns of the drone's body. Different values of distance d (in Equations (1) and (2)) give us different maximum magnitudes of the received signal strength. In the future, how the patterns change vs. distance (observed by received signal strength and phase) will be analyzed. The key challenge here is to find a unique signature on RSS patterns that represents for the effects from the drone body's vibration. We also leave the solution for later investigation.

5. RELATED WORK

Prior work in drone detection includes the following approaches. First, acoustic signature-based detection has been employed for drones. The acoustic signatures of the different drones in the market are collected into a database [6, 5] and compared with the recorded signal to find a match. Noisy urban environments with city traffic pose challenges for using audio for drone detection [4, 10]. Moreover, the database will require constant updating of signatures when new drone models emerge.

Video-based detection methods employ one or more cameras to detect a drone. The live video feed's image is used for analysis to determine if a drone is present or not. Such video-based approaches require costly compute-intensive hardware and/or high bandwidth network connections. Further, using computer image processing to discriminate between other flying objects, e.g. birds, and drones is a challenging task [10]. For night detection, infrared sensing via a thermal camera would be needed [1]. The heat emitted from a drone is used to detect the drone. The effective range to detect humans is around 300m and vehicles is 600m [8]. However, small drones don't produce a lot of heat. One approach combines audio and video-based detection, employing a 120-element microphone array and a video camera to detect and track drones up to 160 to 250 meters, depending on the type [13].

An RF-based detection approach seeks to monitor RF frequency ranges 1MHz - 6.8GHz [3]. Any transmitter that is not known is interpreted as a rogue transmitter or a drone. Such an approach suffers from false positives because unknown RF transmitters are assumed to be a drone even if that is not the case.

Another technique is radar-based detection. Radio waves are transmitted and the reflection from the object is used to verify if it is a drone or not. X-band frequencies are used for the surveillance [9]. Doppler processing of the radar provides the velocity of the target and hence enables the detection of the small moving objects with a low Radar Cross Section. They are passed through a series of electronic filters to distinguish the drone from all the other moving targets [2]. Our active transmission experiments adopt in spirit this approach, with a low cost focus. Radar, audio and optical cameras were combined to track and discriminate airborne targets [31].

Finally, previous work seeks to detect a drone based on its MAC address. In this method, the Parrot drone is detected using the the MAC address along with the individual fingerprints determined by nmap for ports 21,23,5551 and

5555 [25]. The drawback of this method is that we need to maintain a database for all the drones that are manufactured, these ports may be modified and the MAC address could be easily spoofed in order to avoid detection.

6. CONCLUSIONS AND DISCUSSION

This paper has presented a preliminary investigation of drone detection techniques using low cost COTS WiFi and Ettus SDR boards. We have experimentally validated the feasibility of detecting the propeller motion and drone's communication of the drone in the received signal. The effect from drone propeller can be observe from the frequency less than 100Hz. In addition, we found that the eavesdropped signal from the drone and its controller contains distinctive peaks at multiples of 30 Hz in the frequency spectrum. Further, these peaks are distinguishable even in urban environments.

In the future, we plan to expand on this preliminary investigation in a variety of ways. We will explore how to expand the range of detection for both active and passive techniques, such as ways to improve the signal to noise ratio using directional antenna. We will investigate a wider variety of drones over a larger range of RF frequencies. We believe a hybrid approach that combines multiple techniques - passive, active, motion sensing - will be the most robust while remaining cost-effective. In addition, we plan to explore whether the drone can be detected by observing its body vibration through either the active or passive approaches.

7. REFERENCES

[1] Dedrone. http://tinyurl.com/ztfl5v6.
[2] Detect inc. http://tinyurl.com/d3jmkys.
[3] Domestic drone countermeasures. http://www.ddcountermeasures.com/products.html.
[4] Drone detection issues. http://tinyurl.com/gsm4n3t.
[5] Drone detector (orelia). http://tinyurl.com/jcmbmep.
[6] Drone shield. http://tinyurl.com/h4gyahs.
[7] How to shoot down a drone. http://tinyurl.com/p5zaso3.
[8] IEC infrared systems: Banshee. http://tinyurl.com/zeswc7e.
[9] Kelvin Hughes drone detection. http://tinyurl.com/jvxj4kx.
[10] NCC Group. http://tinyurl.com/j8u44sx.
[11] Amazon. Amazon prime air. http://www.amazon.com/b?node=8037720011.
[12] T. Andre et al. Application-driven design of aerial communication networks. *Communications Magazine, IEEE*, 52(5):129–137, 2014.
[13] J. Busset et al. Detection and tracking of drones using advanced acoustic cameras. In *SPIE Security+ Defence*, pages 96470F–96470F. International Society for Optics and Photonics, 2015.
[14] R. Clarke. Understanding the drone epidemic. *Computer Law & Security Review*, 30(3):230–246, 2014.
[15] DJI. DJI Drone. http://www.dji.com/.
[16] J. Geier. 802.11 beacons revealed. *indexed by web. archive. org on Apr*, 17, 2003.
[17] T. HUMPHREYS. Statement on the security threat posed by unmanned aerial systems and possible countermeasures, 2015.
[18] B. Jansen. Drone crash at white house reveals security risks. USA Today, January 26, 2015.
[19] Julio. Parrot bebop quadcopter review: A (near) flawless drone with the skycontroller. http://tinyurl.com/h394ljk. FPV Drone Reviews, February 05, 2016.
[20] Z. Liu et al. Rise of mini-drones: Applications and issues. In *Proceedings of the 2015 Workshop on Privacy-Aware Mobile Computing, ACM MobiHoc*, pages 7–12, 2015.
[21] Mango Communications. Warp v3 kit. https://mangocomm.com/products/kits/warp-v3-kit.
[22] P. McGreevy. Private drones are putting firefighters in 'immediate danger,' california fire official says. LA Times, August 18, 2015.
[23] A. Morrow. Couple accuses neighbor of stalking with drone. USA Today, December 13, 2014.
[24] Parrot. Parrot bebop drone. http://www.parrot.com/products/bebop-drone/.
[25] M. Peacock et al. Towards detection and control of civilian unmanned aerial vehicles. 2013.
[26] S. Piskorski et al. Ar. drone developer guide. *Parrot, sdk*, 1, 2012.
[27] J.-S. Pleban et al. Hacking and securing the ar. drone 2.0 quadcopter: investigations for improving the security of a toy. In *IS&T/SPIE Electronic Imaging*, 2014.
[28] E. Research. USRP B200. https://www.ettus.com/product/details/UB200-KIT.
[29] D. Sathyamoorthy. A review of security threats of unmanned aerial vehicles and mitigation steps.
[30] J. Serna. Lufthansa jet and drone nearly collide near lax. LA Times, March 19, 2016.
[31] W. Shi et al. *Detecting, Tracking, and Identifying Airborne Threats with Netted Sensor Fence*. INTECH Open Access Publisher, 2011.
[32] R. Vander Schaaf. *What technologies or integrating concepts are needed for the US military to counter future missile threats looking out to 2040?* PhD thesis, US Army, 2014.
[33] D. Waldstein. Drone crash interrupts match. New York Times, September 3, 2015.