Defending Against Consumer Drone Privacy Attacks: A Blueprint For A Counter Autonomous Drone Tool

Lanier Watkins*, Shane Sartalamacchia*, Richard Bradt*, Karan Dhareshwar*,
Harsimar Bagga*, William H. Robinson† and Aviel Rubin*
*Johns Hopkins University, USA
†Vanderbilt University, USA

***Abstract*—Drone technology has become ubiquitous, touching almost every aspect of our society. Thus, it is no wonder that malicious actors have now expanded their selfish and criminal pursuits by using drone technology. Currently, these actors commit terrorist acts internationally and domestically, they commit corporate espionage or transport drugs or contraband, and they even violate the privacy of their own neighbors. These are just a few of the many misguided uses of rogue drones. Many researchers in government, corporate, and academia have proposed viable solutions to mitigate the risk associated with this current threat. However, most of these solutions focus on tracking and disrupting the Wi-Fi link between the user and the drone, which may be sufficient for the current threat from Wi-Fi drones, but the future threat is rogue autonomous drones. The use of autonomous drones for rogue purposes poses a more difficult threat to counter since these drones navigate on their own (once given a mission), may not use Wi-Fi at all, and do not require a human in the loop. Given these autonomous drone characteristics, existing user-controlled drone countering tools are ineffective against them and to our knowledge, no other low cost, non-military, and effective counter autonomous drone tools exist. Using DJI drones, which are 74% of the global commercial drone market, in autonomous mode (Active Track), we demonstrate how the use of "hard to patch" vulnerabilities, which break the drone's autonomy code, can be weaponized to design an effective counter autonomous drone tool capable of mitigating one or multiple drones.**

I. Introduction

The drone market is predicted to be $84 billion by 2025. This means that drone technology will begin to surface in every facet of society. Signs of this growing market are all around us. We read and hear news reports regarding positive and negative uses of drones every day. These negative uses center around rogue user-controlled drone contraband delivery, acts of terror locally and abroad, privacy violations and many others. Even though these are unsolved problems, much progress has been made in the form of counter drone tools. However, this problem is further exacerbated when the rogue drones have autonomous capabilities, because little to no progress has been made toward counter autonomous drone tools. Since these drones are not directly controlled by a human operator, the main point (user-to-drone connection) of disruption for existing counter drone tools likely does not exist or is not Wi-Fi. This makes designing and building counter autonomous drone tools fundamentally different from user-controlled counter drone tools and thus the topic we explore in this paper. Our contributions in this paper are: (1) an initial "hard-to-patch" vulnerability assessment (i.e., sensors and wireless network) of two popular COTS autonomous drones (2) design for a novel counter autonomous drone tool. The rest of this paper is organized as follows. In Section 2, we reveal the motivation for our work, and in Section 3 we define our notion of an autonomous drone. Next, in Section 4 we discuss related works, and in Section 5 we discuss DJI's Active Track autonomy. Then, in Section 6 we layout our experimental evaluation, in Section 7 we discuss the results, and in Section 8 we conclude the paper and discuss future work.

Workshop on Decentralized IoT Systems and Security (DISS) 2020
23 February 2020, San Diego, CA, USA
ISBN 1-891562-64-9
https://dx.doi.org/10.14722/diss.2020.23010
www.ndss-symposium.org

II. Motivation

Our paper was motivated by the work done by Birnbach et al. [15] and Watkins et al. [1]. Birnbach et al. in [15] tackled the problem of privacy violation due to a neighbor's user-controlled drone. Essentially, the solution was a counter drone tool with only detection and tracking capabilities. The researchers do an excellent job of implementing and characterizing their solution. The main limitation of their method is a reliance on Wi-Fi for detection, tracking and analysis purposes. Drone technology has evolved greatly since this work was done and now non-Wi-Fi autonomous drones are commercially available (e.g., Phantom 4). This new drone technology now allows for even bolder privacy violations. This motivates us to focus on DJI drones, which is the most innovative drone company, as evidenced by the fact that it controls 74% of the global commercial drone market. Further, in this paper we focus on the DJI Phantom 4 and the Spark, because collectively these drones span the range of autonomous drones features (e.g., Wi-Fi, non-Wi-Fi, infrared-based collision avoidance, vision-based collision avoidance). Essentially, these drones provide us a robust autonomous test-bed.

In Figure 1 a highly likely privacy violation is illustrated. A homeowner has a pool surrounded by a 6 foot privacy fence and teenager daughters who like to host pool parties for their friends. The homeowner has noticed that even though he never sees his neighbor, his neighbor's drone is always flying back and forward on his side of the fence just above the fence's height when the teenagers are at the pool. In this scenario, the autonomous drone has no user controlling it and likely

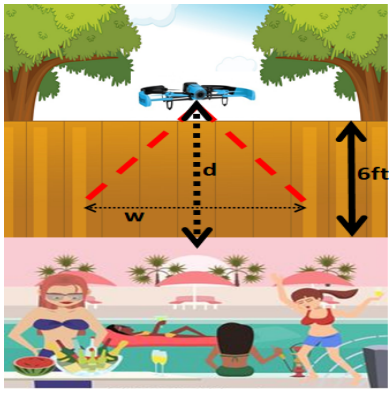

Fig. 1. Privacy Violation Scenario: Neighbor's autonomous drone recording video and flying 6 feet off the ground (just above the shared privacy fence) with a camera viewpoint of width *w* (can capture your entire pool area) and a distance *d* (legally on the neighbor's property) away from the pool area where your teen girls and their friends are swimming. Legally and technically (without our proposed tool), there is nothing the pool owner can do to stop this.

has no Wi-Fi foot print (e.g., DJI Phantom 4 in Active Track mode). This commercially available drone technology would be undetectable and untrackable by the solution proposed by Birnbach et al. and thus could not warn the homeowner of the privacy violation nor stop it. Our work was motivated by this gap in privacy violation mitigation. Similar to Watkins et al. in [1], our tool also uses weaponized "hard-to-patch" vulnerabilities; however, in this work our goal is to track and stop autonomous drones from recording unauthorized video.

III. Notional Autonomous Drone

First, to tackle the differences between a user-controlled drone and an autonomous drone, we must assert that there are different levels of autonomy. According to Ball et al. [5], autonomy can be thought of as having at least 4 levels: (1) Level 0: fully user controlled - manual, (2) Level 1: semi-autonomous (low) - user makes the rules (drone can suggest rules as well) and drone follows them, (3) Level 2: semi-autonomous (high) - drone makes its own rules and user approves them, (4) Level 3: fully autonomous - drone makes its own rules and executes them at will. Also, one important concept to mention in regards to autonomy is emergent behavior, which can be considered a side-effect (e.g., unintended capability, or behavior) that arises due to the interactions of the internal processes within a system. This side-effect is not a consequence of any individual process in the system. For example, temperature and pressure can arise from the interactions of molecules, but temperature and pressure are not specific to any individual molecule [6]. Another example specific to autonomous drones would be a rescue drone that has algorithms to track targets based on color, outline, and can also predict the next movement location of the target; but can also track targets based on size even though it does not have a specific algorithm designed to do so. In this example, the emergent behavior is the ability to track a target by size. This ability arises from the cumulative capabilities of all of the other algorithms working together. In future work, we will be assessing drones with Level 2 and above autonomy, then emergent behavior will be a relevant attack surface to discuss.

A. What Is An Autonomous Drone?

Autonomous drones have the same major parts as user-controlled drones and even more. The "even more" part is namely the mission planner, autonomy, and the emergent behavior associated with the artificial intelligence (AI) in the autonomy. In this section, we only briefly discuss emergent behavior and how it contributes to the overall vulnerability of autonomous drones. This topic will be investigated in more depth in our future work. The reminder of this section will be a discussion of performing an initial vulnerability assessment on the sensors and network of a notional autonomous drone, looking for "hard-to-patch" vulnerabilities as motivated by [1]. These authors assert that these types of vulnerabilities are remotely exploitable and likely will not be patched for the life of the drone, which make good weapons for a counter drone tool.

Our vision of an autonomous drone is illustrated in Figure 2. We see an autonomous drone as having an embedded system that can: (a) communicate with ground stations or other drones via a wireless network, (b) communicate with the drone's rotors, (c) communicate with the drone's sensors (e.g., camera, collision avoidance), and (d) execute autonomy code. This drone can determine its location on Earth using a flight planner or navigational system, which can be a stand-alone system connected to a GPS or additional code running on the embedded system. Also, autonomous drones have a mission planner, which provides an overall goal for the drone. The drone's mission is likely uploaded to it via its ground station, and the drone decides how to accomplish this goal using its autonomy code. We see the COTS DJI Phantom 4 and Spark drones operating in Active Track mode (See Active Track Section below) as real-world examples of Level 1 autonomous drones. The user selects the target to be tracked (i.e., uploads the mission via the controller) and the drone decides how to move around and keep the camera focused on the target, while avoiding any obstacles.

B. Autonomous Drone Security Assessment Versus User-Controlled Drones

As mentioned earlier, an autonomous drone has all of the major components of a user-controlled drone except for the mission planner, autonomy, and flight planner. The Watkins et al. in [1] thoroughly covered the scope of work required to perform a security assessment of user-controlled drones. In this paper we perform an initial vulnerability assessment of autonomous drones by looking mostly at its sensors, wireless network, and GPS. We posit that this is an indirect way of performing a preliminary assessment of the vulnerability of the DJI drone autonomy code. In future work we will fully investigate the vulnerability of other components of autonomous drones, but in this paper we feel that by focusing on a limited set of components from DJI autonomous drones, we can find "hard-to-patch" vulnerabilities, which can be weaponized and used in our design for a counter autonomous drone tool. In comparison to previous vulnerability assessments of user controlled drones, many of our experiments involved over and underwhelming sensors with varying wavelengths of light. To the ill informed, these experiments may appear trivial or pointless; however, these experiments help accomplish our

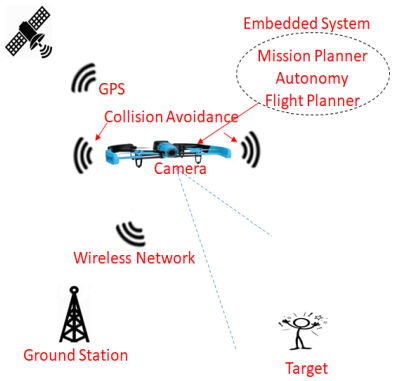

Fig. 2. Notional Autonomous Drone Illustration

goal and provide the necessary insight into "hard-to-patch" vulnerabilities of autonomous commercial drones.

IV. Related Works

To our knowledge, the majority of security assessments and mitigation solutions presented by researchers apply to user-controlled drones. We have only been able to identify short or partial papers that speak to the need for security assessments of autonomous drones.

A. User-Controlled Drone Security Assessments

Watkins et al. in [1] and Hooper et al. in [2] attempted to simplify the process of assessing the security of user-controlled drones by focusing their penetration testing efforts on the major components of these drones. The researchers break commercial off the shelf (COTS) drones into 4 components: wireless network, GPS, navigational system, and embedded system. Specifically, Watkins et al. in [1] focused on performing a security assessment of multi-vendor drones, finding vulnerabilities and weaponizing these vulnerabilities to produce a counter drone tool. In contrast, Hopper in [2] focused on demonstrating the vulnerability of a popular COTS drone and proposing a mitigation solution.

B. Autonomous Drone Security Assessment

Apvrille et al. in [4] described the possibility of using a SysML-Sec environment for mitigating the risks associated with security and privacy while developing embedded systems such as autonomous drones. According to the authors, this platform has previously demonstrated success in autonomous vehicle development. They posited that this platform would be able to support requirements elicitation, attack capture, hardware/software partitioning, and software design during the development process. Other than modeling, this platform is currently supported by the TTool open-source toolkit that enables formal verification of safety and performance properties from partitioning diagrams and safety and security properties from design diagrams. Apvrille et al. in [4] used this platform with a Parrot drone, which was infused with autonomous capabilities. It it hard to gauge the overall contribution of this platform since to our knowledge no Parrot drones have inherent autonomous capabilities; whereas, in this paper we illustrate an initial security assessment on the inherently autonomous DJI Spark using Active Track.

V. DJI Active Track and Autonomy

Based on the definition put forth in the previous section, user-controlled drones are Level 0, and COTS autonomous drones, like the DJI Spark and Phantom 4, are Level 1 semi-autonomous (low). In other words, the DJI Spark and the Phantom 4 when put into autonomous mode can make its own video recording decisions based on a set of rules established by the user.

Active Track (ATrak) is a feature provided by DJI that allows a user to select a subject from the frame of the camera of the drone, and the drone then follows and records the subject. The drone intelligently tracks the subject by using its vision and sensing systems to fly safely while the target can be engaged in any physical activity, such as walking down a path, driving on the road, or swimming in the ocean. DJI uses its own proprietary algorithm for Active Track coupled with a few other libraries, such as 'KCPcpp', which is a target tracking library based on Kernelized Correction Filter, and 'YOLO V2', which is a state-of-the-art, real-time object detection system. Active Track offers two features. One enables the drone to track a target from either front or back, or even circle around the target, and another enables the drone to track a target from a fixed perspective set by the user. The drone detects the target automatically, but it also detects how fast the target is moving, and the drone moves accordingly [9] [10].

A. DJI Phantom 4

The DJI Phantom 4 (P4) is a large drone that can be utilized in a commercial or hobbyist environment. This drone is equipped with advanced technology to enable it to track objects autonomously while avoiding obstacles in its way. It achieves this capability through its ATrak technology and its obstacle avoidance sensing system. The Phantom 4's vision positioning system (VPS) has a maximum range of 33 feet. A user interfaces with the Phantom 4 through the DJI GO 4 application installed on a smartphone. This smartphone is connected to the Phantom 4 remote controller via a USB cable. The controller is not WiFi-based, so this drone and many others can fly and stream video back to its controller without the use of WiFi. The Phantom 4 includes GPS, Global Navigation Satellite System (GLONASS), two front optical sensors, two bottom optical sensors, one camera, two ultrasonic sensors, gyroscope, and two Inertial Measurement Unit (IMUs) [12].

B. DJI Spark

DJI Spark is one of the new smaller sized drones being offered by DJI. It has intelligent flight control options like QuickShot (Professional Videos with a single tap), TapFly (making the drone fly to a particular spot with a single tap on the screen), ATrak (Tracking a target) and Gesture Control. It has a mechanical gimbal and a camera capable of HD video recording and 12 MP photos. With features like Return to Home and Intelligent battery, the drone ensures that it returns home safely when it nears its total flight time of 16 minutes. The primary interface for the Spark uses touch controls through the DJI GO 4 application installed on a smartphone. The Spark has its own WiFi network to which the smartphone needs to connect to allow wireless controls and video streaming. The drone has one camera and three infrared sensors - one on the

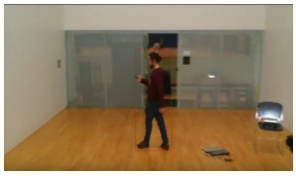

Fig. 3. Normal ATrak Autonomy

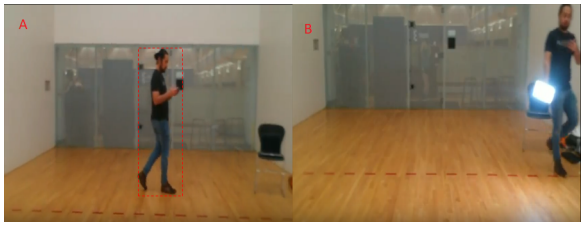

Fig. 4. ATrak Autonomy disrupted by Bright Light Attack

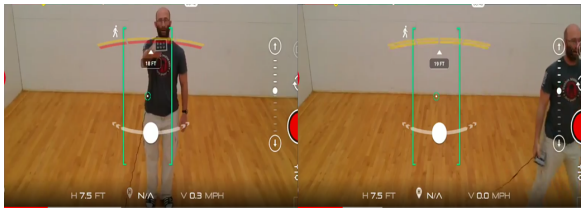

Fig. 5. ATrak Autonomy disrupted by Infrared Sensor Level Attack

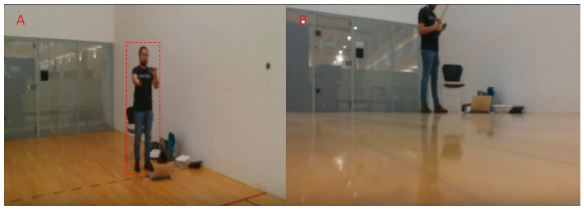

Fig. 6. ATrak Autonomy disrupted by GPS Attack

front and two on the bottom of the device. Additionally, the drone also has inbuilt GEO system that keeps track of all the restricted flying zones in the area and prevents the drone from flying in zones that can raise safety or security concerns [7] [13].

VI. Experimental Evaluation

In this paper, we perform an initial security assessment on the sensors, wireless network, and GPS of the DJI Phantom 4 and Spark drones looking for "hard-to-patch" vulnerabilities. We see the DJI Phantom 4 and Spark as exemplar COTS autonomous drones. We then demonstrate how weaponized "hard-to-patch" vulnerabilities can be used to design a counter autonomous drone tool that can track and disrupt the video recording and tracking of a target.

A. Experimental Setup

Our experimental setup consisted of two drones, DJI Phantom 4 and Spark. We also used an attack laptop running Kali Linux, HackRF One, 1.5-foot Yagi 1.58 GHz antenna, smartphone running DJI-Go application, 1,220 Lux (held at 3 meters) LED Floodlight, a similar LED Floodlight, which

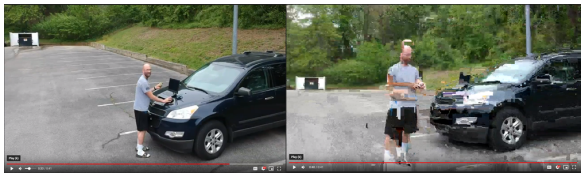

Fig. 7. ATrak Autonomy disrupted by Wireless Deauthentication Attack

could change colors, and an 850 nm wavelength infrared spotlight (held at 3 meters) composed of 6 LEDs.

B. Experimental Procedure

In our experimental procedure, we focused on assessing the vulnerability of the DJI Phantom 4 and Spark drones looking for "hard-to-patch" vulnerabilities. Specifically, we investigated: (1) the vulnerability of the drones' optical and infrared sensors to denial of service attacks and (2) the vulnerability of the drones' autonomy to inherent real-time operating system (RTOS) interrupts due to the wireless network and GPS attacks.

1) Optical Sensor Attack: First, we launched the DJI Spark and then the Phantom 4 (on a separate occasion) in Active Track mode and trained it on a human target. This target moved around and viewed the DJI-GO application screen on the smartphone to ensure that the drones were able to track it. Then we landed the drones and downloaded their flight plans to establish a baseline.

Then, again we launched the DJI Spark and then the Phantom 4 in Active Track mode and trained it on a human target. This target moved around and viewed the DJI-GO application screen on the smartphone to ensure that the drones were able to track it. Then we had the target to point a bright LED Floodlight (situated 3 meters away) toward the DJI Spark and Phantom 4 using different intensities (one third, one half, and full 1,220 Lux intensity) and also using different colors (e.g., blue, red, green, white) and observed the results. Finally, we downloaded the flight plan from the DJI drones and analyzed them.

2) Infrared Sensor Attack: Next, we launched the DJI Spark and then the Phantom 4 in Active Track mode and trained it on a human target. This target moved around and viewed the DJI-GO application screen on the smartphone to ensure that the drone was able to track the target. Then we had the target point an infrared spotlight toward the DJI Spark and Phantom 4 and observed the results. Next, we downloaded the flight plan from the DJI drones and analyzed them.

3) Embedded System Interrupt Attack: Again, we launched the DJI Spark and Phantom 4 in Active Track mode and trained it on a human target. Next the target used a HackRF One to spoof the location of the drone to that of the U.S. White House and observed the result. Then, we downloaded the flight plan from the DJI drones and analyzed them. Next the target used Kali Linux aircrack suite of tools to deauthenticate the autonomous drones from their controller (ground station) and observed the result. Then, we downloaded the flight plan from the DJI drones and analyzed them.

TABLE I. ATRAK FLIGHT PLAN EXPERIMENTAL DATA

Experiment	OSD.ctrl Device	OSD.flight Action	OSD.fly cState	APP WARN
Baseline	Onboard Device	None	NaviSubModeTracking	
Optical	RC	None	GPS_Atti	Subject Lost
Infrared	RC	None	GPS_Atti	
GPS	RC	Airpt	AutoLanding	NoFly Zone
Wireless Deauth	RC	GoHme	AutoLanding	

Data Published At: https://zenodo.org/record/3634048#.XjchDMhKiUk

VII. RESULTS AND DISCUSSION

We used the flight plan that was downloaded from the first experiment to serve as a baseline for the other experiments. An illustration of the autonomous tracking capability of the DJI Spark is shown in Figure 3. Note the drone records and keeps the target in the center of the frame when tracking. The drone stops recording and the target appears elsewhere in the video frame when Active Track fails. Also, Table 1 - Row 1 reveals that the drone itself knows that it is being controlled (column **OSD.ctrldevice**) by an on-board device and it is currently flying and tracking (column **OSD.flycState**) a target, not taking any specific action (column **OSD.flightAction**) and it is not under any duress (column **APP.WARN.warn**).

A. Autonomy Code Vulnerability to Optical Sensor Attack

From these experiments, we have determined that the color of the light does not matter for both the Phantom 4 and Spark, only the intensity. The full intensity of the LED Floodlight using any color we tested, up to 3 meters away causes the DJI Spark and Phantom 4 to stop tracking and recording its target. This result is captured in Figure 4. In Figure 4A, the DJI Spark illustrates the ability to track its target; however, when the target points the LED floodlight towards the drone, it loses its ability to track and record the target and the target consequently walks away (In Figure 4B target is no longer in the center of the window). Note, in contrast to the baseline mentioned previously, this experiment is capable of causing duress to the drones' autonomy (Active Tracking) as evidenced by Figure 4 and Table 1 - Row 2 where the flight plan reveals that the target was lost and the control mechanism abruptly changed (GPS_Atti denotes an abrupt change in control device [11]).

B. Autonomy Code Vulnerability to Infrared Sensor Attack

From these experiments, we have determined that it is possible to overwhelm the infrared sensor as well. The Figure 5 and Table 1 - Row 3 both indicate that the DJI Spark and Phantom 4 stop tracking and recording their target when the infrared (IR) spotlight is used. In Figure 5A, the DJI Spark (Phantom 4 does not have infrared sensors) illustrates the ability to record and track its target; however, when the target points the infrared spotlight towards the drone, it loses its ability to record and track the target and the target consequently walks away (See Figure 5B). In Table 1 - Row 3 the flight plan reveals that the control mechanism of the drone abruptly changed.

C. Autonomy Code Vulnerability to System-level Interrupts

From these experiments, we have determined that the DJI Phanton 4 and Spark's autonomy code (Active Track) and recording can be subverted by spoofing the location of the drone to an unauthorized location such as the U.S. White House. The Spark's autonomy can also be subverted by severing the connection between the drone and its controller or ground station (Phantom 4 does not use WiFi, so the WiFi-based de-authentication attack does not work). It is known that the drone's RTOS continuously monitors the GPS coordinates checking to ensure that the drone is not at an airport or other restricted areas (e.g., the U.S. White House). This is known as geofencing [16], but until these experiments there was no certainty that geofencing would subvert the autonomy code. Apparently, the RTOS also continuously monitors the wireless link to the controller to ensure that it is up as well. In Figure 6a the drone illustrates the ability to record and track its target, but after the target attacks the GPS and tricks the drone into thinking it is flying over the U.S. White House, the drone forces (likely via an interrupt) itself to stop recording and tracking its target and lands (See Figure 6b). All of this is corroborated by Table 1 - Row 4 where the flight plan reveals that the drone thinks it is in a no fly zone at an airport, and will be auto landing. The target spoofs the GPS and the drone forces itself to land, thus subverting its autonomous mode. Similarly, for the Spark in Figure 7a the drone illustrates the ability to record and track its target, but after the target attacks the wireless network and severs the drone from its controller (ground station) the drone forces (likely via interrupt) itself to stop recording and tracking its target and lands (See Figure 7B). Notice the picture in Figure 7B is now very close to the ground and it also starts to get grainy. This is the last image sent from the drone just before the connection is broken. All of this is corroborated by Table 1 - Row 5 where the flight plan reveals that the drone is flying back to home and then auto landing.

D. Counter Autonomous Drone Tool Design

The Table 2 below summarizes the vulnerabilities found during our security assessment of the sensors, wireless network, and GPS of the DJI Phantom 4 and Spark autonomous drones. We consider all of these vulnerabilities as "hard-to-patch", and we have confirmed with DJI that they do not plan to patch any of these. Their logic was that they do not think these vulnerabilities pose any harm to drone users, and only time can verify their logic. Having said that, some of these vulnerabilities could be weaponized and used to counter autonomous drones, which would provide a solution to privacy violation risks such as the one illustrated in Figure 1.

1) Architecture: A counter autonomous drone tool could be developed by mounting a Hack RF One and a 1,220 Lux spotlight on an antenna dish that has two degrees of freedom, azimuth and elevation. The 0 – 360 degree rotation (azimuth) and the 0 – 90 degree up and down (elevation) movements could be driven by stepper motors designed to locate the strongest 2.4GHz signal (both DJI Spark-WiFi and Phantom 4-non-WiFi drones use this frequency). This mechanism basically uses the Hack RF One to hone in on the strongest signal for a drone's controller channel. While not used to control the Spark or Phantom 4, the controllers for both

drones are used to receive streamed video. Since this behavior is common for both Wi-Fi and non-WiFi-based drones, the controller's wireless channel to the drone can be leveraged as a means to detect autonomous drones.

2) Major Design Challenge: Note, normal Wi-Fi for computer networks operate in the 2.4GHz frequency band as well as the DJI drones. Therefore, one of the major design challenges is to discern between normal Wi-Fi for computer networks and DJI drone usage in this frequency range. We believe this can be done by focusing on the identification of the DJI drone broad peak at 2.45GHz (P4 and Spark), which is not used by Wi-Fi for computer networks, see Figure 8. The details of doing this is beyond the scope of this paper, but will be investigated in future work.

3) Operation: Once a drone is detected, the Spoofed GPS (forces drone to land) or the 1,220 Lux White Light (drone hovers) vulnerabilities can be exploited to break the autonomous tracking of the drone. This tool could be used to counter the privacy violation mentioned earlier and illustrated in Figure 1. This tool should work with any of the DJI autonomous drones, which accounts for 74% of the entire global commercial drone market [14].

4) Limitations: Our design is restricted in its range of effectiveness, because of the effective range of our tested exploits. Based on our experiments: (1) the 850nm IR and 1,220 Lux White Light Attacks were effective up to a range of 3 meters, (2) the GPS Spoofing Attack was effective up to 3 meters away, and (3) the wireless De-authentication Attack was effective up to 20 meters away. We believe that the effective range can be increased by using a brighter LED white light, an amplified IR spotlight, or a better Hack RF One antenna design.

VIII. Summary and Future Work

In this paper, we offer a design for a novel counter autonomous drone tool based on the weaponization of "hard-to-patch" vulnerabilities (DJI confirmed they will not patch these vulnerabilities) found while performing an initial security assessment of the sensors and wireless network of the DJI Spark and Phantom 4 drones. This counter autonomous drone tool fills a critical need for mitigation of risks due to privacy violations of the type illustrated in Figure 1. This tool targets DJI drones, which are 74% of the global drone market. In future work, we plan to build this tool and test its capabilities and limitations. One of the largest challenges will be discerning between Wi-Fi for computer networks and DJI wireless controller traffic.

TABLE II. Summary of Autonomous Drone Vulnerabilities

Drone	Component	Vulnerability	Range	Behavior
P4/Spark	Optical Sensor	1,220 Lux White Light	$\leq 3m*$	Breaks Autonomy Code and Hovers
P4/Spark	GPS	GPS Spoofing	$\leq 3m@$	Breaks Autonomy Code and Lands
Spark	Wireless Network	Wi-Fi Deauth.	$\leq 20m$	Break Autonomy Code and Lands
Spark	IR Sensor	850nm IR Light	$\leq 3m*$	Breaks Autonomy Code and Hovers

*Extended by increasing intensity
@Extended by using better antenna

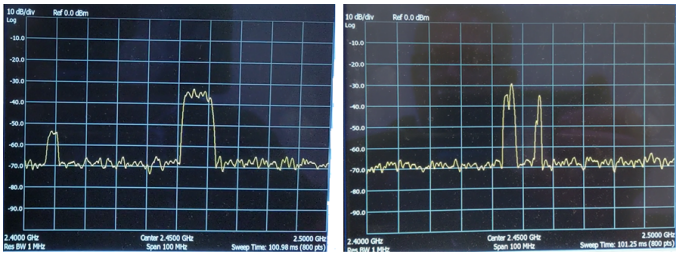

Fig. 8. Snapshot of Phantom 4 wireless 2.4GHz-2.5GHz spectrum versus Wi-Fi: Over a 1 minute observation window, Left-Phantom 4 spectrum is mostly dominated by one single static broad peak with dynamic narrower peaks, Right-Wi-Fi spectrum mostly has only several dynamic narrower peaks

References

[1] L. Watkins, J. Ramos, G. Snow, J. Vallejo, Wi.H. Robinson, A.D. Rubin, J. Ciocco, F. Jedrzejewski, J. Liu, and C. Li, "Exploiting Multi-Vendor Vulnerabilities as Back-Doors to Counter the Threat of Rogue Small Unmanned Aerial Systems," In ACM Proceedings of the MobiHoc Workshop on Mobile IoT Sensing, Security, and Privacy, June 26, 2018.

[2] M. Hooper , Y. Tian, R. Zhou, B. Cao, A.P. Lauf, L. Watkins, W.H. Robinson, and W. Alexis, "Securing Commercial WiFi-Based UAVs From Common Security Attacks," In IEEE MILCOM 2016, Baltimore, MD, November ,2016.

[3] M. Juang,"Drone entrepreneurs take flight as costs fall and money-making rises",Available At: https://www.cnbc.com/2017/06/17/3-ways-you-can-turn-flying-drones-into-a-money-making-job.html , June 2017.

[4] L. Apvrille, Y. Roudier, T. Tanzi, "Autonomous drones for disasters management: Safety and security verifications", In URSI Atlantic Radio Science Conference, 2015.

[5] M. Ball, V. Callaghan, "Perceptions of Autonomy: A Survey of User Opinions towards Autonomy in Intelligent Environments", In IEEE International Conference on Intelligent Environments, 2011.

[6] L. Steele, "The Artificial Life Roots of Artificial Intelligence" Artificial Life Journal Vol. 1 pg 75-110, 1994..

[7] DJI Official. (2018). DJI Spark – Selfie Drone – DJI. [online] Available At: https://www.dji.com/spark.

[8] Flylitchi.com. (2018). Litchi for DJI Mavic / Phantom / Inspire / Spark. [online] Available at: https://flylitchi.com/.

[9] Developer.dji.com. (2018). Advanced Sensing - Object Detection Sample - DJI Onboard SDK Documentation. [online] Available at: https://developer.dji.com/onboard-sdk/documentation/sample-doc/advanced-sensing-object-detection.html.

[10] Developer.dji.com. (2018). Advanced Sensing Target Tracking Sample DJI Onboard SDK Documentation. Available at: https://developer.dji.com/onboard-sdk/documentation/sample-doc/advanced-sensing-target-tracking.html.

[11] DJI Forum Website, Available At: https://forum.dji.com/thread-100626-1-1.html.

[12] Phantom 4 User Manual, Available: https://dl.djicdn.com/downloads/phantom_4/20170706/Phantom_4_User_Manual_v1.6.pdf

[13] Spark User Manual, Available: https://dl.djicdn.com/downloads/Spark/Spark%20User%20Manual%20V1.6-.pdf

[14] Dronelife.com. (2018) "New Report Unveils Drone Industry Market Share Figures", Available: https://dronelife.com/2018/09/18/new-report-unveils-drone-industry-market-share-figures/

[15] S. Birnbach, R. Baker, and I. Martinovic, "Wi-Fly?: Detecting Privacy Invasion Attacks by Consumer Drones," Network and Distributed System Security Symposium (NDSS), February, 2017.

[16] DJI Website on Geofencing, Available At: https://www.dji.com/newsroom/news/dji-refines-geofencing-to-enhance-airport-safety-clarify-restrictions.