Poster: Enabling Secure Location Authentication in Drone

Feng Xiao, Man Zhou, Youcheng Liye, Jingxiao Yang, Qian Wang
{f3i,zhouman,liye97,yangjingxiao,qianwang}@whu.edu.cn
The State Key Lab of Software Engineering, School of Computer Science, Wuhan University, P. R. China

ABSTRACT

With the popularity of commodity drones in a wide variety of applications, significant security issues have been raised. One of the major problems is that a legal drone may be illegally hijacked by GPS spoofing attacks. Though some GPS anti-spoofing techniques have been proposed, no effective technique has been implemented in commodity drones yet due to practical limitations. Motivated by the ubiquitous WiFi signals around us, we propose WiDrone, a WiFi fingerprint location cross-check based anti-hijacking system on commodity drones in this poster. WiDrone still relies on GPS for navigation but it will authenticate the destination by comparing current WiFi fingerprint (CWF) with the destination WiFi fingerprint (DWF) when the drone receives a landing order. Furthermore, we propose a WiFi fingerprint authentication algorithm to decide whether CWF matches DWF. We have designed and implemented the prototype of WiDrone on DJI Matrice 100 to ascertain the practicability of proposed system.

CCS CONCEPTS

• **Security and privacy** → **Mobile and wireless security**; • **Networks** → **Location based services**;

KEYWORDS

Drone, Secure Location Authentication, WiFi

1 INTRODUCTION

Drones (or unmanned aerial vehicles) are aircraft without pilots on board. With the fast development of drone technology, commodity drones have been increasingly used in a wide variety of applications, such as aerial photography, search and rescue, environmental monitoring, electrical inspection and so on. In recent years, some e-commerce giants have proposed to employ drones for delivery services of packages (e.g., Amazon Prime Air [2] and JD.com Drone Delivery Program [3]). It is widely believed that the drone industry will experience an exponential growth in the near future.

However, the popularity of drones also raises a number of security issues. One of the major problems is that a legal drone may be illegally hijacked by adversaries. For example, an adversary may hijack the delivery drone on its way to the destination and take away the packages. The easy implementation of hijack mainly because drones only rely on civilian GPS navigation while civilian signals are not encrypted or authenticated. In civilian GPS, the signals are spread using publicly known spreading codes. Therefore, the adversary can cheat the drone's GPS receiver by broadcasting bogus signals (called GPS spoofing attacks [6]) and control the drone landing on the way. Researchers have shown how to successfully spoof GPS receivers of drones with COTS (commercial off-the-shelf) GPS signal simulator or software defined radios [1, 4, 8].

Some proposed GPS anti-spoofing techniques recently can be classified into four categories: signal processing defenses, cryptographic defenses, correlation with other GNSS sources and radio spectrum and antenna defenses [5]. These countermeasures monitor GPS signals and detect the abnormality, modify on satellite to encrypt civilian signals, cross-check with other timing or location sources, or use customized antenna receiver. However, due to some practical limitations, no effective technique has been implemented in commodity drones yet. Motivated by the ubiquitous WiFi signals around us, we propose WiDrone, an anti-hijacking system on commodity drones which leverages the WiFi fingerprint for location cross-check in this poster. WiDrone still relies upon GPS for navigation but it will authenticate the destination by comparing current WiFi fingerprint with that of the destination before the drone starts to land. We have designed and implemented the prototype of WiDrone on DJI Matrice 100 to ascertain the practicability of proposed system. Video of the conducted case study can be found in [9].

2 SYSTEM DESIGN

In this section, we present the design of WiDrone. To enable anti-hijacking on commodity drones which systems are always restricted and unprogrammable, it is crucial to build an extensible onboard platform that is able to authenticate the destination as well as automatically control the drone. Hence, we propose WiDrone, the extensible anti-hijacking platform for drones. Figure 1 elaborates the architecture of the proposed design.

Design goal. The goal of WiDrone is to protect drones from GPS-spoofing attack with WiFi fingerprint. Currently, there are two methods to spoof drone: 1) No-fly zone abuse: The firmware of commodity drones records the GPS information of areas over which drones are not permitted to fly, and these locations are called No-fly zone. Emitting No-fly zone GPS information might lead drones to fly back or land immediately. 2) Fine-grained GPS spoofing: Attackers emit false GPS

MobiCom '17, October 16–20, 2017, Snowbird, UT, USA

ACM ISBN 978-1-4503-4916-1/17/10.
https://doi.org/10.1145/3117811.3131259

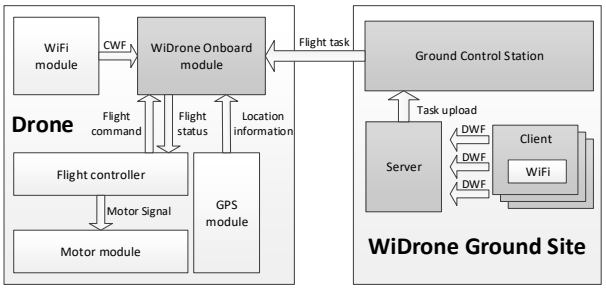

Figure 1: System architecture of WiDrone.

(a) DJI Matrice 100

(b) USRP

Figure 2: (a) is the drone prototype used in WiDrone, (b) is the GPS spoofing tool.

signals that slightly different from the real one, so as to gradually mislead the drone to the false location. The first one is not efficient because it is easy to be detected: Since legitimate flight routines will not fly over any no-fly zone, such attacks need to emit GPS signals that are far away from any location in the routine. Hence drones can easily detect the spoofing. In our poster, WiDrone mainly focuses on the fine-grained GPS spoofing, which is more efficient and commonly used [1].

WiDrone workflow. As shown in Figure 1, a user firstly submits an order along with its destination WiFi fingerprint via the client (e.g., a mobile app), then the server will gather orders from the user and submit them to the ground control station of drones. After the onboard platform receives the flight task with the destination WiFi fingerprint (DWF) from the ground site, it will navigate the vehicle to the destination.

Once WiDrone judges that it arrives at the destination according to GPS location information, it will perform the authentication algorithm in the air, to authenticate the destination by current WiFi fingerprint(CWF), and CWF only records the RSSI of APs. If CWF matches DWF, it will touch down and finish the task. Otherwise, it will decide that errors or attacks occur in the GPS locating, and thus climbs to a safe flying height and flies away from the wrong location. After that, it will be navigated by GPS module and perform the same authentication before landing.

Core algorithm design. The algorithm of WiDrone addresses two major challenges. First, unlike previous works [10] about high accuracy localization, WiDrone needs to perform the algorithm high from the air. The signals are very weak. In addition, objects in the city (e.g., bird, tree and car) can exert strong interference on the WiFi signals. However, our goal is to achieve high accuracy and robustness so that an attacker near the true destination could not hijack the drone. To achieve this goal, we employ WiFi fingerprint set V_d and V_c to describe DWF and CWF. All APs and its corresponding Received Signal Strength Indication (RSSI) are recorded ($V_d = \{Rd_1, Rd_2, ..., Rd_\alpha\}$, $V_c = \{Rc_1, Rc_2, ..., Rc_\beta\}$).

Even though APs are ubiquitous in the cities, they are sometimes unstable: Any AP near the destination can be established or removed at any time. To overcome this challenge, Client of WiDrone will ask the user to submit the latest DWF periodically. For example, a user who wants to deliver some goods to his side can submit the order with WiDrone mobile client, the client will collect DWF immediately. In addition, users can save some common delivery addresses in advance when they are at that place so that they can deliver goods from everywhere.

When drones are about to arrive at the destination, it will detect the CWF and calculate the WiFi fingerprint similarity s between V_d and V_c. We compute $V_u = V_d \bigcup V_c$, and thus obtain $V_u = \{Rd_1, Rd_2, ..., Rd_\varphi\}$. If there is an element in V_u that is not in V_d, corresponding element will be added into V_d and its value will be set to 0. The same operations will be performed on the set V_c. Then the number of elements in V_d and V_c will all be φ. Let R_{max} denote the max value of RSSI, and s is calculated as follows

$$s = 1 - \frac{\sum_{i=1}^{\varphi} |Rd_i - Rc_i| \cdot Rd_i / R_{max}}{\sum_{i=1}^{\varphi} Rd_i^2 / R_{max}} \quad (1)$$

If s is larger than a threshold, WiDrone will permit the drones to land at the destination.

3 SECURITY ANALYSIS

WiDrone leverages AP fingerprint to achieve secure authentication before landing. Unlike civil GPS that are unencrypted and unauthenticated, APs can be encrypted. To cheat WiFi based location authentication system [7], attackers can only perform replay attack to counterfeit APs as well as jam original WiFi signals locally to avoid leaking genuine location information. However, WiFi jamming can be easily detected. Since cities are full of public/private APs, such jamming is unavoidable if attackers want to capture the drone flying in cities. To further mitigate such attacks, WiDrone can ask users to establish a temporary AP specialized for WiDrone authentication (e.g., personal hotspot on mobile phones), and then WiDrone performs secure landing by authenticating and connecting to this special AP.

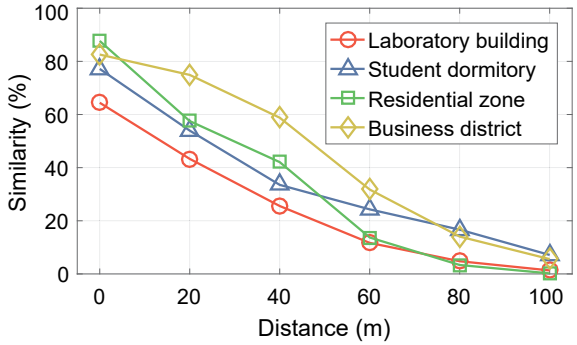

Figure 3: The WiFi fingerprint similarity s in different environment.

4 EVALUATION

4.1 Experiment Setup

In this poster, we implement our system on DJI Matrice 100. The core onboard module is implemented on a Raspberry Pi 3. We choose MT7601U wireless network card as the WiFi module to perform WiFi fingerprint collection. The Drone and the Raspberry Pi was connected via UART cable. Figure 2(a) shows our system, and we use USRP N210 as the GPS spoofing tool, as shown in Figure 2(b).

4.2 Result

To guarantee the usability of our system, we must ensure that WiDrone can accurately authenticate the CWF with DWF. Since drones will sample CWF in the air while DWF is always sampled on the ground or at indoor environments, the influence of distance between CWF and DWF on similarity is critical. Hence, we investigate the relationship of distance and similarity s in our algorithm. We conducted an experiment in which our drone is at different distance from the destination with a horizontal interval of ten meters and a total of 100 meters.

We choose four typical destinations for drones to validate our algorithm: a plaza in front of the laboratory building, a street between student dormitory, area inside residential zones and business districts. First, we collect DWF on the ground at the four places, and then we sample CWF from different distances above destinations. Figure 3 illustrates the relationship between fingerprint similarity and distance. As shown in Figure 3, s declines when the distance becomes larger. All four lines can be roughly divided into 2 periods: When the distance is less than 60 meters, declines are more rapid, however, declines becomes slower after 60 meters. This is because WiDrone will collect many other fingerprints that are not in DWF from 60 meters away that add up noises into similarity calculation, thus s becomes less sensitive with distance. To perform secure authentication, we should choose the distance in the first period where different WiFi fingerprints can be accurately differentiated. Hence we set the authentication distance at 50 meters, where WiDrone is able to authenticate WiFi fingerprints at all typical destinations. We deem that 50m is a suitable distance to perform authentication since sampling CWF from DWF 50m away can satisfy most landing scenarios in the cities.

5 CONCLUSION AND FUTURE WORK

In this poster, we designed and implemented WiDrone, an anti-hijacking system on commodity drones which leverages the WiFi fingerprint for location cross-check. The authentication algorithm is effective with our design, and its mitigation against spoofing attack is demonstrated. The design of WiDrone leverages WiFi infrastructure to perform city location authentication, and we deem that such design is stable enough because WiFi signals are ubiquitous in cities. However, it may fail to finish some special tasks if we wish WiDrone lands in particular scenarios (e.g., a mountain area without enough WiFi signals). In the future, we plan to add more kinds of signals (e.g., FM radio signals, GPRS signals) into consideration and design a dynamic algorithm to adaptively combine some of them to perform more robust authentication. The applications of WiDrone is not limited to the applications depicted in this paper but can be further expanded. For example, there is a growing concern that malicious drones may give rise to terrorist attacks or illegal spying by bypassing no-fly zone policy. WiDrone may provide a secure and low-cost solution against these problems (e.g., No-fly WiFi zone can be introduced in our further works).

6 ACKNOWLEDGMENT

Qian's research is supported in part by National Natural Science Foundation of China under Grant No. 61373167, National Basic Research Program of China under Grant No. 2014CB340600.

REFERENCES

[1] Researchers successfully spoof an 80-million yacht at sea, 2013. https://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea.
[2] Amazon prime air, 2016. https://www.amazon.com/b?node=8037720011.
[3] Jd.com drone delivery program, 2016. http://fortune.com/2016/11/14/jd-china-drone-delivery-singles-day/.
[4] Huang, L., and Yang, Q. Low cost gps simulator: Gps spoofing by sdr. *DEFCON* (2015).
[5] Schmidt, D., Radke, K., Camtepe, S., Foo, E., and Ren, M. A survey and analysis of the gnss spoofing threat and countermeasures. *ACM Computing Surveys (CSUR) 48*, 4 (2016), 64.
[6] Tippenhauer, N. O., Pöpper, C., Rasmussen, K. B., and Capkun, S. On the requirements for successful gps spoofing attacks. In *Proc. of CCS* (2011), ACM, pp. 75–86.
[7] Tippenhauer, N. O., Rasmussen, K. B., Pöpper, C., and Capkun, S. Attacks on public wlan-based positioning systems. In *Proc. of MobiSys* (2009), ACM, pp. 29–40.
[8] Wang, K., Chen, S., and Pan, A. Time and position spoofing with open source projects. *Black Hat Europe 148* (2015).
[9] Xiao, F., Zhou, M., Liye, Y., Yang, J., and Wang, Q. Poster: Enabling secure location authentication in drone. https://youtu.be/T1mA9tRDVz0.
[10] Yang, Z., Wu, C., and Liu, Y. Locating in fingerprint space: wireless indoor localization with little human intervention. In *Proc. of MobiCom* (2012), ACM, pp. 269–280.