드론을 이용한 비행 중 침입 탐지에 대한 연구

유하[*], 정창훈[*], 양대헌[*]
[*]인하대학교 컴퓨터공학과
e-mail:rymy_eetu@hotmail.com

A Study of Flying Intrusion Detector using the Drone

Lumme Juha[*], Changhun Jung[*], DaeHun Nyang[*]
[*]Dept of Computer Science, Inha University

Abstract

We argue that the one potential solution is creating a drone or quadcopter that could be used to detect the network hacking attempts and even have the capability to disconnect illegal drones from their user's jamming signals, or de-authenticate them from networks. This could be used as a direct countermeasure, or would at least provide monitoring capacities, for these criminally-purposed drones. In this paper, we focus on implementing the device that can detect intrusion.

1. Introduction

These days there are many heated discussions regarding drones due to the increasing number of illegal purposes for which they are being used. Drones are now being frequently used for wireless network hacking attempts, mobile phone hacking attempts[1], spying and other criminal activities. We can see a common theme among news stories[2-4] regarding drones being used for hacking, and this has recently been spreading at an alarming rate[3-5]. From this substantial number of news reports, we can conclude that drone-based hacking has now become a significant threat that may become devastating[4, 6] in the next few years if left unchecked[3, 4]. So, now the question becomes whether or not there is a way to neutralize this threat before it becomes an unavoidable consequence of advancing technology.

At the Black Hat security conference 2014 in Singapore, information security firm SensePost introduced Snoopy[7], a drone that can hack into Wi-Fi and steal the data from those networks. Snoopy is also able impersonate a network that an unsuspecting user might join, whereupon the code would steal that user's data. This method could be used to particular effect in a crowded environment where many people have their cell phones automatically searching for Wi-Fi networks. We can see more and more spreading news about drones used hacking and the news numbering drone based hacking next big threat. The question is, if there is a way to avoid such threats somehow.

How about making drones being able to detect this kind of attempts. Moreover, could drones be disconnected from users jamming signals or de-authenticate untrusted signals from network? It would be the more interesting if drones can be used countermeasure or monitor those attempts.

We argue that the one potential solution is creating a drone or quadcopter that could be used to detect these kinds of attempts and even have the capability to disconnect these illegal drones from their user's jamming signals, or de-authenticate them from networks. This could be used as a direct countermeasure, or would at least provide monitoring capacities, for these criminally-purposed drones.

In this paper, we focus on implementing the device that can detect intrusion. To implementation, we use a Raspberry Pi 3B, Kali Linux and WaidPS. Also we check whether if our device could be combined with drone and we draw a flowchart from our project by assuming it.

The remainder of this paper is organized into 4 sections. Section 2 describes that related work we used to implement our device. Section 3 describes our study and project. Experimental results are presented in Section 4. The conclusion is drawn in Section 5.

2. Related work

In this section we review hardware and software needed to build working detection device.

2.1 Raspberry Pi 3B

Raspberry Pi 3B is Microcomputer with 1GB RAM, 4 USB 2.0 ports and BCM2837 1.2Ghz quad-core processor, wireless LAN and Bluetooth 4.0. Raspberry Pi 3B would be used as the heart of the intrusion detection module. Since it is a small and low power usage computer, however, it does not come without any problems. It has limited processing power, so the handling of generated detection lists is not fast, especially if there is a substantial amount of wireless devices in the scanning area. In order to make Raspberry Pi 3B to work in the way it is intended, we need to concentrate on optimizing the used code and lighten the used operating system in the future by removing all unnecessary applications and routines from it. We also need use a external battery to supply power to Raspberry Pi 3B, Wi-Fi dongle(for packet injection) and a MicroSD card to store required software and scanning results. Thus we need consider weight of Raspberry Pi with needed external battery, Wi-Fi dongle and MicroSD card, because Drones payload capacity is limited and extra weight shorten drone fly time.

<Table 1> Weights of used hardware

Used hardware	Weight
Raspberry Pi 3B kit	50.2g
Samsung 32Gb MicroSD card	0.5g
TP-Link TL-WN722N USB Wi-Fi dongle	45g
USB Battery Xiaomi 5000MaH	156g

Table 1 above shows weights of used components, therefore we need use drone that can support 251.7g. It is lightweight enough to be carried in common quadcopters, like Parrot AR Drone 2.0 which maximum payload is 450 grams, but that is future work.

2.2 WaidPS

WaidPS is a Python programming language based on an open source program made to run in the Linux environment. It is a wireless Swiss knife-style, multipurpose tool designed for wireless network penetration testing. In addition to this, it also collects all Wi-Fi information in the surrounding area and stores that collected data into its own databases. This method will be useful when it comes to auditing a network if the access point is considered "MAC filtered" or "hidden SSID", meaning there is no existing client at that moment. The primary purpose of this script is to detect intrusion, but its uses reach far beyond this goal. Once wireless hacking is detected, it displays the data onscreen as well as logging this file of the attack into its database.

We use WaidPS on Kali Linux in Raspberry Pi 3B to detect some hacking attempts. Before we are able to run and use WaidPS, we need install some required software upon Kali Linux operating system. Needed software's are Python programming language module(at least version 2.7), Aircrack-NG suite(Tools to assess Wi-Fi network security), TShark(Network protocol analyzer) and TCPDump(packet analyzer) installed. Also we need install Mergecap(if we want use joining for pcap files) and Wi-Fi Harvesting Module(to analyze all the surround traffic). The Raspberry Pi 3B will be strong enough to run Kali Linux with WaidPS with Python programming language module, Tshark, Aircrack-NG suite, TCPDump and Mergecap.

3. A Study of Flying Intrusion Detector using the Drone

The very beginning of the project, we needed examine the hardware and software needed in order to make this project possible. The drone itself is not included here because the first step that needs to be completed is the creation of a micro-computer system module in order to test if it can be made lightweight and small enough to be carried by a specific drone. First point of our study was to see if we can make working and lightweight enough detection device which will be able to install in drone. After that we are able to continue our study and install made detection device into the drone.

The very core of this project setup is centered on Raspberry Pi 3B, which has an attached MicroSD card. This would be powered by a USB power bank that acts as an external battery, and Kali Linux was chosen as the operating system because it is designed to penetration testing. Basic distro have all unnecessary applications ripped off. A TP-Link N722 USB adapter would be plugged into one of the four USB ports and used for packet injections. Since this device would require a substantial amount of storage space, a 32GB MicroSD card would be used for the storage of all the needed software and files. For further reference, Fig 1 is setup for our device and a general image of how all the parts are to be connected and used together. It's weight is about 252g. It is lightweight enough to be applied into a drone.

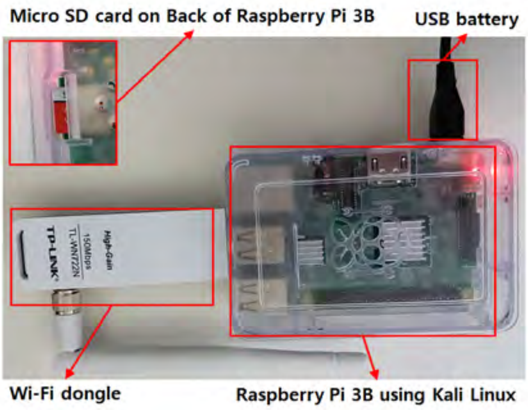

Micro SD card on Back of Raspberry Pi 3B
USB battery
Wi-Fi dongle
Raspberry Pi 3B using Kali Linux

Fig 1 Setup for our device

To our work, we added some function into WaidPS on Kali Linux. Additional features that have been added to the current script that were not found in the previous are as follows: (ⅰ) automatically save the attack packets into a file, (ⅱ) interactive mode where users are allowed to perform many functions, (ⅲ) allow user to analyze captured packets, (ⅳ) customizable filters, (ⅴ) customize detection threshold (sensitivity of IDS in detection). At this point our interest is being able to detect the following wireless attacks: (ⅰ) Evil-Twin, (ⅱ) Rogue Access Point. Once wireless hacking is detected, it displays the data on screen as well as logging this file of the attack into its database.

We assume that we can combine the our device with drone in future, so we made a flowchart of our final study(project). Please refer to Fig 2.

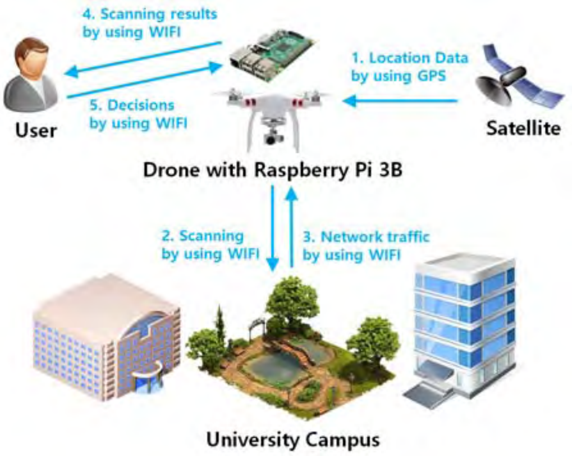

4. Scanning results by using WIFI
User
5. Decisions by using WIFI
1. Location Data by using GPS
Satellite
Drone with Raspberry Pi 3B
2. Scanning by using WIFI
3. Network traffic by using WIFI
University Campus

Fig 2 Flowchart for a study of flying intrusion detector using the drone

At first(1), drone with our device can receive a GPS signal to patrol pre-designed route in campus, second(2), drone with our device will scan the network in campus. Third(3), monitoring wireless network traffic using Wi-Fi with harvesting module to detect any potential threat. Fourth(4), when it detect possible attempts, it will categorize these activities by threat type and record all necessary information required to identify the exact threat and infecting device. Then it generate report file and send results to user. Fifth(5), user can then determine if the threat is a false alarm or actual threat. User can then choose next action.

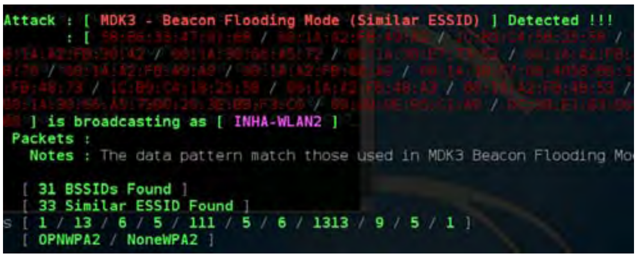
4. Experiment

In Section 2, we examined the hardware and software needed in order to make this project possible. The drone itself is not included here because the first step that needs to be completed is the creation of a micro-computer system module in order to test if it can be made lightweight and small enough to be carried by a specific drone.

We built a detection device, as mentioned before, that was centered on Raspberry Pi 3B and installed all the necessary software into it. Once all the software was updated and adjusted, we were finally able to test whether or not WaidPS was able to do its job properly and detect intrusions as detailed in this paper.

We tested our detection device walking around Inha University campus to see if it is able to detect any possible evil twins and rogue access points successfully. By walking around we were able to simulate drone and its possible flight route. The why we test in University Campus area, University Campus is ideal testing area because there is lot of wireless access points with many different networks and there is also lots of wireless device users like students with their mobile devices.

WaidPS proved to be a useful program script when it was tested to detect possible threats. The program is designed to use penetration testing and invasion detecting, and it was able to recognize possible evil twin and rogue access points during our experiment like Fig 3 and create useful log files regarding these threats. We could see WaidPS terminal of Kali Linux on our device through remote desktop program like Fig 3. Fig 3 mean that 31 Mac Address have a similar ESSID also have same name INHA-WLAN2, our device detected them.



```
Attack : [ MDK3 - Beacon Flooding Mode (Similar ESSID) ] Detected !!!
       : [ [illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible] ] is broadcasting as [ INHA-WLAN2 ]
 Packets :
   Notes : The data pattern match those used in MDK3 Beacon Flooding Mo

   [ 31 BSSIDs Found ]
   [ 33 Similar ESSID Found ]
s  [ 1 / 13 / 6 / 5 / 111 / 5 / 6 / 1313 / 9 / 5 / 1 ]
   [ OPNWPA2 / NoneWPA2 ]
```

Fig 3 Experiment result

Script have much more possibilities like detect passive mode have sniffing Wi-Fi cards, Association / Authentication flooding, Possible WPS attack using the ARP request replay method, Detect possible WEP attack using chopchop method, Detect possible WPS pin brute force attack by Reaver, Bully, and others.

In actual test we did not use drone but walk around Campus area with our detection device. Device was able to detect possible evil twin and rogue access points.

5. Conclusion and Future Work

During this project we were able to see issues related to the security of drones and the potential threats they pose. As mentioned in the introduction, these security issues created through the expansion of drone usage is becoming more well-known in the public sector through various media reports. For this reason, without any prior knowledge, we attempted to create and test a drone that is able to detect hijacking attempts and perform needed countermeasures or other actions. We successfully created a portable credit-card sized computer system, which works with a small external battery independently which can be mounted on the drone.

Today, the so-called "digital arms race" is expected to continue indefinitely, assuming Moore's law is still valid in the world of computing. This ultimately means that our computing power in any given economy will be doubled nearly every other year.

The security threats that we mentioned before can be resolved in several ways. In order to protect commercial networks and prevent them from being hacked, companies should set up safer Wi-Fi networks for their signal transmission. Also, nearly every household has a wireless router providing their private internet connection. Based on this law, we can observe that the rapid rate of computing power development leads average users to keep upgrading their personal electronic devices to the newer versions. This means that end user level computers are expected to become much more powerful in a short period of time.

Applying this concept to our project, we can conclude that we will likely see even more powerful and smaller computers, such as the one we utilized, available in the market. This means it will become even faster and easier to hack wireless networks and it will be even more necessary to create drones that are able to neutralize these threats.

In the future work, we hope to extend our work and create an actual autonomously flying defender drone that is capable of independently detecting possible threats and monitoring them. Also, adding a feature that could made a triangle measurement form the attacker wireless signal source, would allow us to use video cameras, making a live-feed of the attacker. We also may need charging station for drones to extend their operating time. This also give us opportunity to research possible wireless charging station installations near patrolling route.

References

[1] M. Kumar, “Drones Spying on Cell Phone Users for Advertisers,” The Hacker News, Mar. 2015, http://thehackernews.com/2015/03/drone-cell-phone-spy.html.

[2] H. Kuchler, “Cyber experts warn of hacking capability of drones,” Financial Times, Jul. 2016, https://www.ft.com/content/a06a1f5c-505f-11e6-8172-e39ecd3b86fc.

[3] J. Nicas, “Criminals, Terrorists Find Uses for Drones, Raising Concerns,” The Wall Street Journal, Jan. 2015, https://www.wsj.com/articles/criminals-terrorists-find-uses-for-drones-raising-concerns-1422494268.

[4] J. Lima, “Drone hacking is the next big threat,” Computer Business Review, Aug. 2015, http://www.cbronline.com/news/internet-of-things/smart-technology/disturbing-military-policies-ground-the-potential-of-drones-4650937

[5] “The Next Great Threat From Hackers: Drones?,” Mar. 2016, http://www.ozy.com/fast-forward/the-next-great-threat-from-hackers-drones/67660

[6] J. Lowy, “FAA contemplating whether millions of drones will fill skies,” PHYS ORG, Sep. 2016, https://phys.org/news/2016-09-faa-contemplating-millions-drones.html

[7] D. Storm, “Flying spy: Snoopy drone helps hackers steal data from your phone,” Computer World from IDG, Mar. 2016. http://www.computerworld.com/article/2476048/cybercrime-hacking/flying-spy--snoopy-drone-helps-hackers-steal-data-from-your-phone.html