Poster: Wireless Access Point Spoofing by Unmanned Aerial Vehicles (UAVs)

Ryota Kawakami, Atsuo Inomata, Naoto Yanai and Toru Fujiwara
Osaka University

***Abstract*—Considering threats by unmanned aerial vehicles (UAVs) is an important direction for security community. In this paper, we propose wireless access point spoofing by UAVs. We also show a proof-of-concept implementation via an experiment and discuss potential threats by UAVs.**

I. Introduction

An unmanned aerial vehicle (UAV) is originally an aircraft that moves without any human pilot on board, and is also known as a drone. Nowadays, information security is a serious issue for UAVs and there are two standpoints for security researches, i.e., *attacks to UAVs* and *attacks by UAVs*. In this paper, we focus on attack methods by UAVs, that are few in the early literature. According to some existing work [1] about attacks by UAVs, there is also a potential risk of privacy whereby an attacker can fly an UAV over walls in order to surveil the inside of a building via those cameras.

In this work, we propose a network device spoofing method by UAVs as a new aspect of attack by UAVs. While spoofing itself is a major kind of attack for network security, an attacker can set any spoofed device on anywhere by combining with the use of UAVs: more specifically, the attacker can fly UAVs even over walls by virtue of their maneuverability. Furthermore, since UAVs are set even in the outside of a building, UAVs are also able to spoof network devices without any physical access to the building. Consequently, our finding attack is able to make more target espionages than the conventional spoofing, i.e., spoofing without UAVs, and thus will become a more serious threat in future. We also show a proof-of-concept (PoC) implementation. With our finding, we raise security awareness about potential threats by UAVs within the academic community and the industrial society for information security.

II. Threats of Unmanned Aerial Vehicles

Although several threats against UAVs have been found according to Fotouhi et al. [2], we focus on attacks where an attacker can arbitrarily control UAVs and execute to attack from blind spots, e.g., through walls. In particular, UAVs may try network device spoofing, e.g., a router or a wireless access point, in order to reveal information without being detected. Based on the background, we are motivated to lead clients connected with the legitimate network device to connect with UAVs provided by an attacker without any physical attack or destruction of the network device itself. To establish such a threat, we need the three following assumptions. 1) An attacker knows some kind of access information such as SSID of the target device and its password. 2) UAVs are allowed to have access on the premises where the target exists. 3) An attacker is required to use commercially available UAVs. Fig. 1 is an example of an attack flow based on our scenario. The attacker can also own and control plural UAVs against any target.

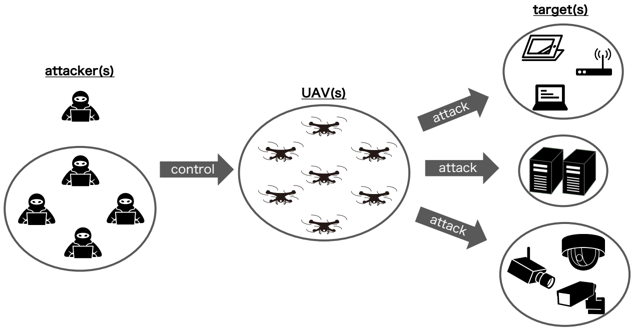


Fig. 1: Example of Threats by UAVs

III. Wireless Access Points Spoofing by Unmanned Aerial Vehicles

In this section, we propose an attack method for wireless access point spoofing by a UAV. First, an attacker utilizes a UAV, which provides network interfaces and whose shell on UAV's operating system is enabled. When the attacker needs to set any file into the UAV, the attacker sends them through the network interfaces and then runs them in the shell. Next, the attacker sets the same SSID and its password to the UAV as those of the wireless access point to establish a connection of the UAV with its local network. The attacker then sets an IP address of the UAV to the same address of the wireless access point. Hence, The UAV is able to spoof the target wireless access point. Consequently, the UAV misleads clients, who want to (re)connect with the local network, to connection with the UAV itself instead of the wireless access point.

IV. Experiment

We conduct an experiment to evaluate a PoC implementation of the proposed attack method. In this experiment, for the simplicity we utilize one UAV and suppose that WAN of an access point is disabled. In doing so, the UAV spoofs a wireless access point with the arp spoofing. Fig. 2 shows our experimental environment. We share the detail about the

Network and Distributed Systems Security (NDSS) Symposium 2020
23-26 February 2020, San Diego, CA, USA
ISBN 1-891562-61-4
https://dx.doi.org/10.14722/ndss.2020.23xxx
www.ndss-symposium.org

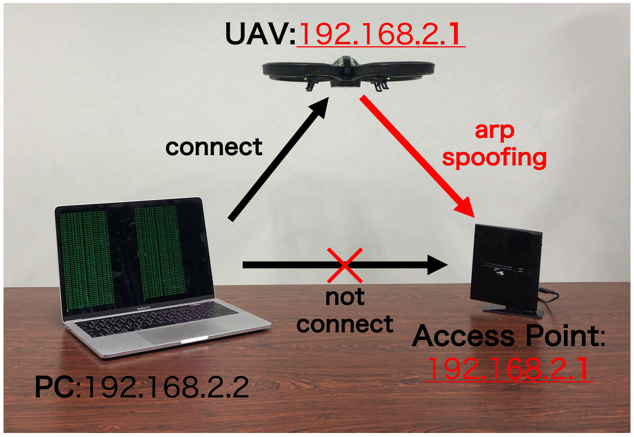
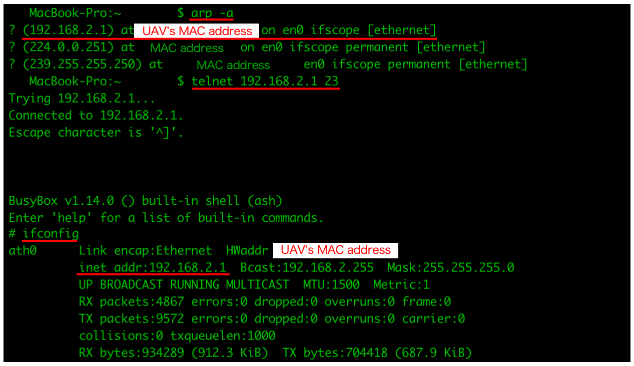


Fig. 2: Experimental Environment



```
   MacBook-Pro:~        $ arp -a
? (192.168.2.1) at UAV's MAC address on en0 ifscope [ethernet]
? (224.0.0.251) at  MAC address  on en0 ifscope permanent [ethernet]
? (239.255.255.250) at    MAC address    en0 ifscope permanent [ethernet]
   MacBook-Pro:~        $ telnet 192.168.2.1 23
Trying 192.168.2.1...
Connected to 192.168.2.1.
Escape character is '^]'.



BusyBox v1.14.0 () built-in shell (ash)
Enter 'help' for a list of built-in commands.
# ifconfig
ath0      Link encap:Ethernet  HWaddr UAV's MAC address
          inet addr:192.168.2.1  Bcast:192.168.2.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4867 errors:0 dropped:0 overruns:0 frame:0
          TX packets:9572 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:934289 (912.3 KiB)  TX bytes:704418 (687.9 KiB)
```

Fig. 3: Result of Wireless Access Point Spoofing

experiment of the proposed attack on request for research use.

Experimental Environment: At the beginning of the experiment, the target local network of a wireless access point is different from that of the UAV. Meanwhile, an attacker knows an SSID and a password of the wireless access point from the assumptions described in Section II. The UAV in the experiment was originally unable to deal with WPA2. Hence, we sent "wpa_supplicant", "wpa_cli", and "wpa_passphrase" to the UAV via ftp, and then run them in the UAV's shell.

Result: As shown in Fig. 3, a connection of the UAV is established to the wireless access point with an IP address which is the same as the target. Next, we check if either one of the UAV or the wireless access point owns the address of "192.168.2.1" through a MAC address from an arp table of the laptop in Fig. 2. When the MAC address is identical to that of the UAV, the arp spoofing is succeeded, that is, the UAV is successful for spoofing the wireless access point.

According to the arp table of the laptop, "192.168.2.1" was owned by the UAV. Besides, by executing the telnet command from the laptop to confirm more certainly, we confirmed that the laptop was connected to the UAV. Based on these results, we confirmed that the UAV is able to spoof the wireless access point in this experimental environment.

V. Discussion

We discuss consideration based on the experiment below.

Further Threats: First, we consider that UAVs can also become routers by installing files related to the capability of the routers. Likewise, by utilizing file server spoofing, UAVs may be able to become a file server within the target network and then can transfer the communicated data to another file sever owned by an attacker. We consider that our attack is available for spoofing on many kinds of network device. Next, we consider the use of multiple UAVs for attacks on a single wireless access point as a target. In doing so, these UAVs are closed to the target, and then one of the UAVs which is able to provide a strong signal forces clients in the target network to connect with the UAV itself. Moreover, by utilizing multiple channels, an attacker can set multiple access points. Accordingly, a user will becomes indistinguishable about a legitimate wireless access point and that of the UAVs.

Economics and Ethics: We used a cheap and commercially available UAV. This implies that anyone can try our attacks and is potentially able to create a heavy damage and threat. Here, we want to note that our experiment was conducted in the local network in our laboratory. Thus, the experiment is legal because we did not attack anything outside of the laboratory network.

Countermeasures: Finally, we discuss countermeasures against the proposed attack. Intuitively, if a user can confirm the integrity of information sent from each wireless access point, spoofing by UAVs can be prevented. Although the use of an authentication mechanism such as digital signatures is known as the conventional tools, the use of blockchains has been proposed in [3] to guarantee the integrity and transparency of data provided from each device including UAVs. Another countermeasure is to detect UAVs themselves. According to Birnbacha et al. [1], UAVs are potentially detectable by checking those signal strength. Introducing these approaches may be able to mitigate threats by UAVs.

VI. Conclusion

We conclude that UAVs are able to succeed in network device spoofing. In doing so, by virtue of the maneuverability of UAVs, our finding attack becomes more serious and severe threats than spoofing without UAVs in the conventional attacks. In future work, we plan to discuss the router spoofing and the countermeasures described above.

Acknowledgment: This work was supported by JSPS KAKENHI Grant Numbers JP17K00192 and Innovation Platform for Society 5.0 at MEXT.

References

[1] S. Birnbach, R. Baker, and I. Martinovic, "Wi-fly?: Detecting privacy invasion attacks by consumer drones," in *Proc. of NDSS 2017*. Internet Society, 2017.

[2] A. Fotouhi, H. Qiang, M. Ding, M. Hassan, L. G. Giordano, A. Garcia-Rodriguez, and J. Yuan, "Survey on uav cellular communications: Practical aspects, standardization advancements, regulation, and security challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3417–3442, 2019.

[3] S. Aggarwal, M. Shojafar, N. Kumar, and M. Conti, "A new secure data dissemination model in internet of drones," in *Proc. of ICC 2019*. IEEE, 2019.

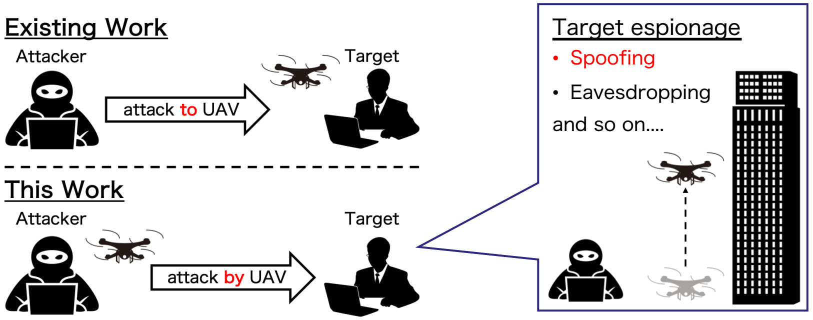
Wireless Access Point Spoofing by Unmanned Aerial Vehicles (UAVs)

Ryota Kawakami, Atsuo Inomata, Naoto Yanai, Toru Fujiwara (Osaka University) r-kawakami@ist.osaka-u.ac.jp

OSAKA UNIVERSITY

Introduction

✓ Information security is a serious issue for UAVs .
✓ Two standpoints of research: *attacks to UAVs* or *attacks by UAVs.*
✓ Propose a network device spoofing method by UAVs as a new aspect of attacks by them.
✓ Raise security awareness about potential threats of UAVs.



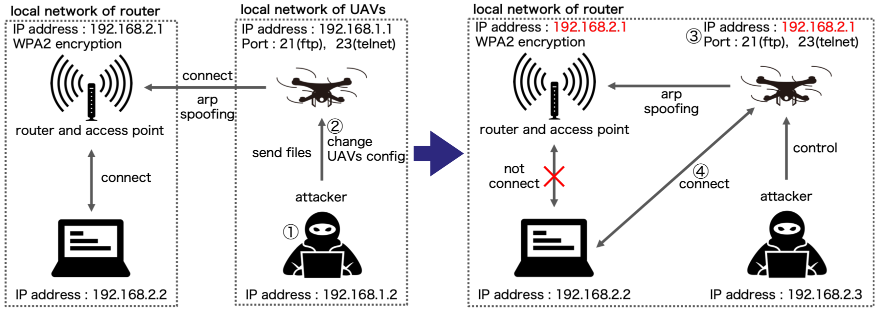
Proposed Attack

Assumption

1. An attacker knows some kind of access information such as SSID of the target device and its password beforehand.
2. UAVs can have access on the premises where the target exists.
3. The attacker is required to use commercially available UAVs.

Wireless Access Points Spoofing by UAVs

Step1: Enable to the shell on UAVs' operating system.
Step2: Set the same SSID and password to UAVs as those of the wireless access point to connect with the target LAN.
Step3: Set the same IP address of the UAVs as that of the wireless AP.
Step4: Spoof the wireless access point and mislead clients into UAVs.

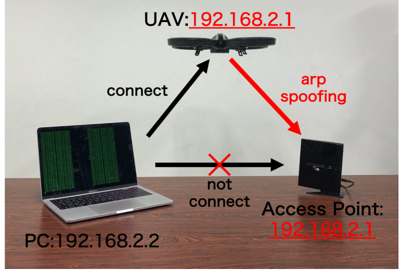


[1] S. Birnbach, R, Baker, and I. Martinovic, "Wi-Fly?: Detecting privacy invasion attacks by consumer drones", NDSS 2017.
[2] S. Aggarwal, M. Shojafar, N. Kumar, and M. Conti, "A new secure data dissemination model in internet of drones", ICC 2019.

Experiment

Experimental Purpose

Show a PoC implementation of our proposed attack.

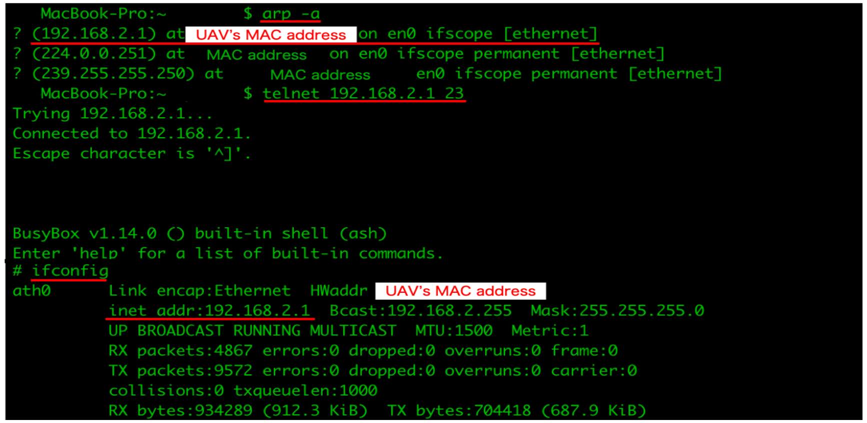


Experimental Environment

Look the right-side picture.
✓ Utilize one UAV for simplicity.
✓ WAN of an access point is disabled for simplicity.
✓ The target local network of a wireless access point is different from that of the UAV.
✓ An attacker knows an SSID and a password of the wireless access point from the assumptions.
✓ Send 3 files related to WPA2 via ftp and run in the shell.

Result

According to the arp table of the laptop, "192.168.2.1" of IP address was owned by the UAV. Then, confirm that the shell of the UAV can be entered by using telnet to the UAV.



```
   MacBook-Pro:~          $ arp -a
? (192.168.2.1) at UAV's MAC address on en0 ifscope [ethernet]
? (224.0.0.251) at  MAC address  on en0 ifscope permanent [ethernet]
? (239.255.255.250) at     MAC address     en0 ifscope permanent [ethernet]
   MacBook-Pro:~          $ telnet 192.168.2.1 23
Trying 192.168.2.1...
Connected to 192.168.2.1.
Escape character is '^]'.



BusyBox v1.14.0 () built-in shell (ash)
Enter 'help' for a list of built-in commands.
# ifconfig
ath0      Link encap:Ethernet  HWaddr UAV's MAC address
          inet addr:192.168.2.1  Bcast:192.168.2.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4867 errors:0 dropped:0 overruns:0 frame:0
          TX packets:9572 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:934289 (912.3 KiB)  TX bytes:704418 (687.9 KiB)
```

Discussion

From the Result

✓ UAVs can also become other network devices, e.g., routers.
✓ To connect more certainly, multiple UAVs can be used.

Countermeasures

✓ Detect UAVs by checking those signal strength [1].
✓ Use blockchains to guarantee data integrity and transparency [2].

Ethics: Our experiment was conducted in the local network in our lab. and thus is legal because of no attack outside.