A Systematic Threat Analysis and Practical Attacks on Automated Frequency Coordination Systems

Yilu Dong[†], Tianchang Yang[†], Arupjyoti Bhuyan[◊], Syed Rafiul Hussain[†]

† *The Pennsylvania State University*

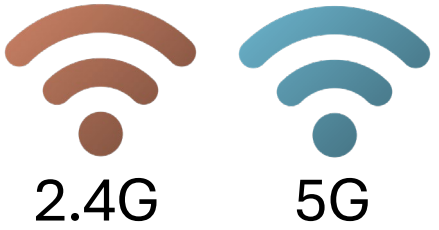
◊ *Idaho National Laboratory*

PennState

Idaho National Laboratory

Why is AFC Critical for 6 GHz?

Legacy 2.4 GHz and 5 GHz Wi-Fi systems are already congested

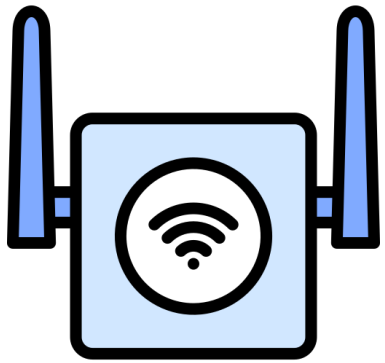


This new 6 GHz spectrum is already used by mission-critical incumbent systems

The **Automated Frequency Coordination** (AFC) system manages spectrum access and prevents interference

Fixed Service Links

- ❑ Point-to-point wireless links
- ❑ Operate in same the 6 GHz bands
- ❑ Incumbents protected by AFC



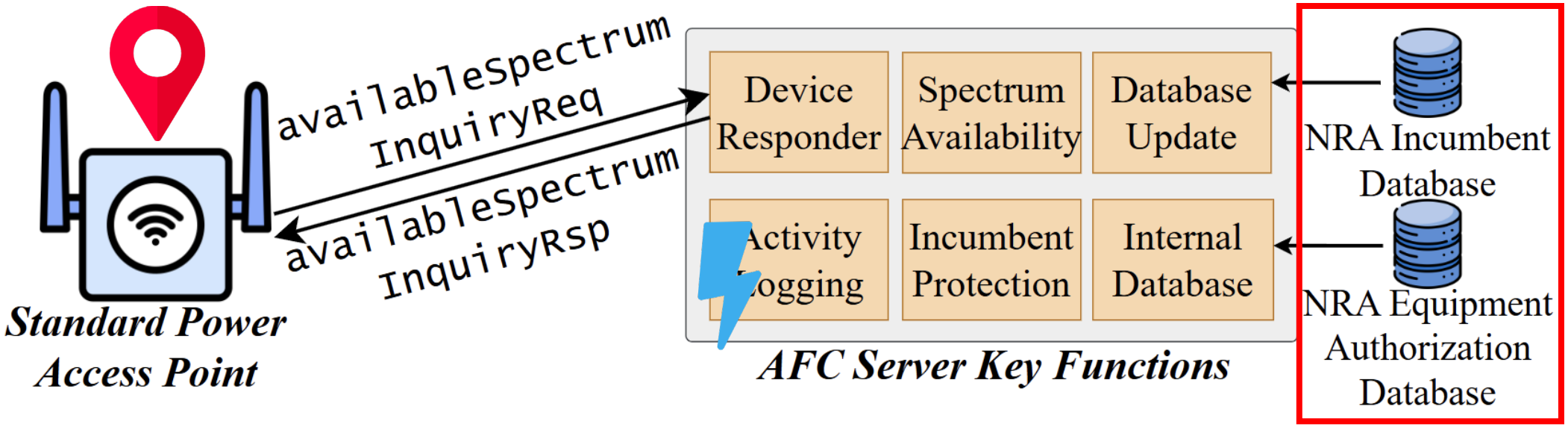
SP AP

Interfere

Fixed Link/Incumbent

Automated Frequency Coordination System

AFC system coordinates the spectrum for Wi-Fi APs
to avoid interference with incumbents.



Simplifying Spectrum Sharing

Citizens Broadband Radio Service (CBRS)

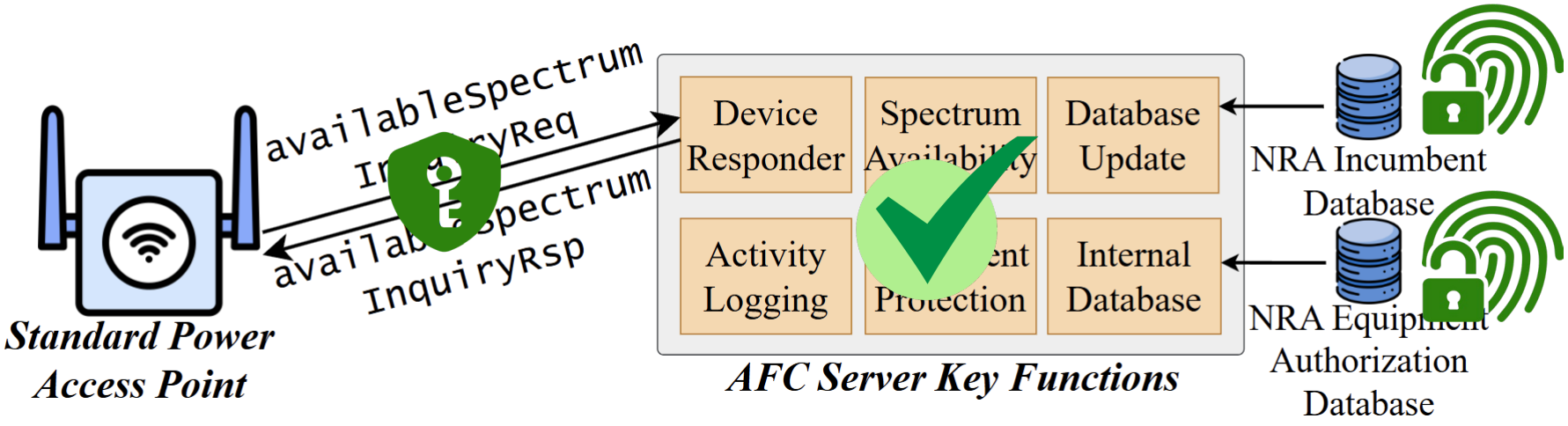
Professional Installer

Spectrum Sensing

Operator Coordination

General Security Requirements of AFC System

- ***REQ1***. **Mutual Authentication** between the AP and server.
- ***REQ2***. **Integrity** of internal AFC databases
- ***REQ3***. **Accurate Interference Protection** on AFC server

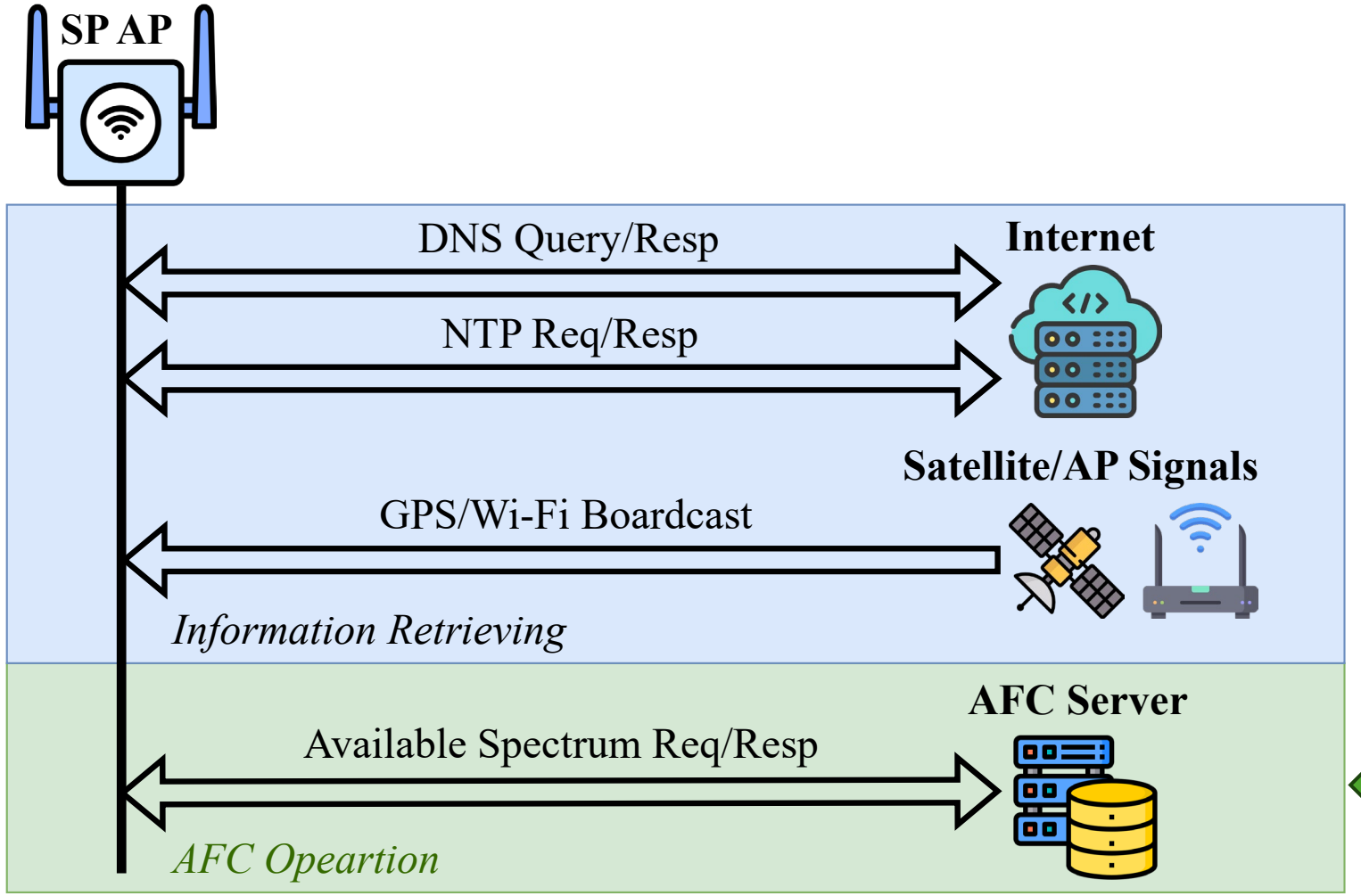


Are these requirements enough to keep the AFC system function as intended?

Threat Model

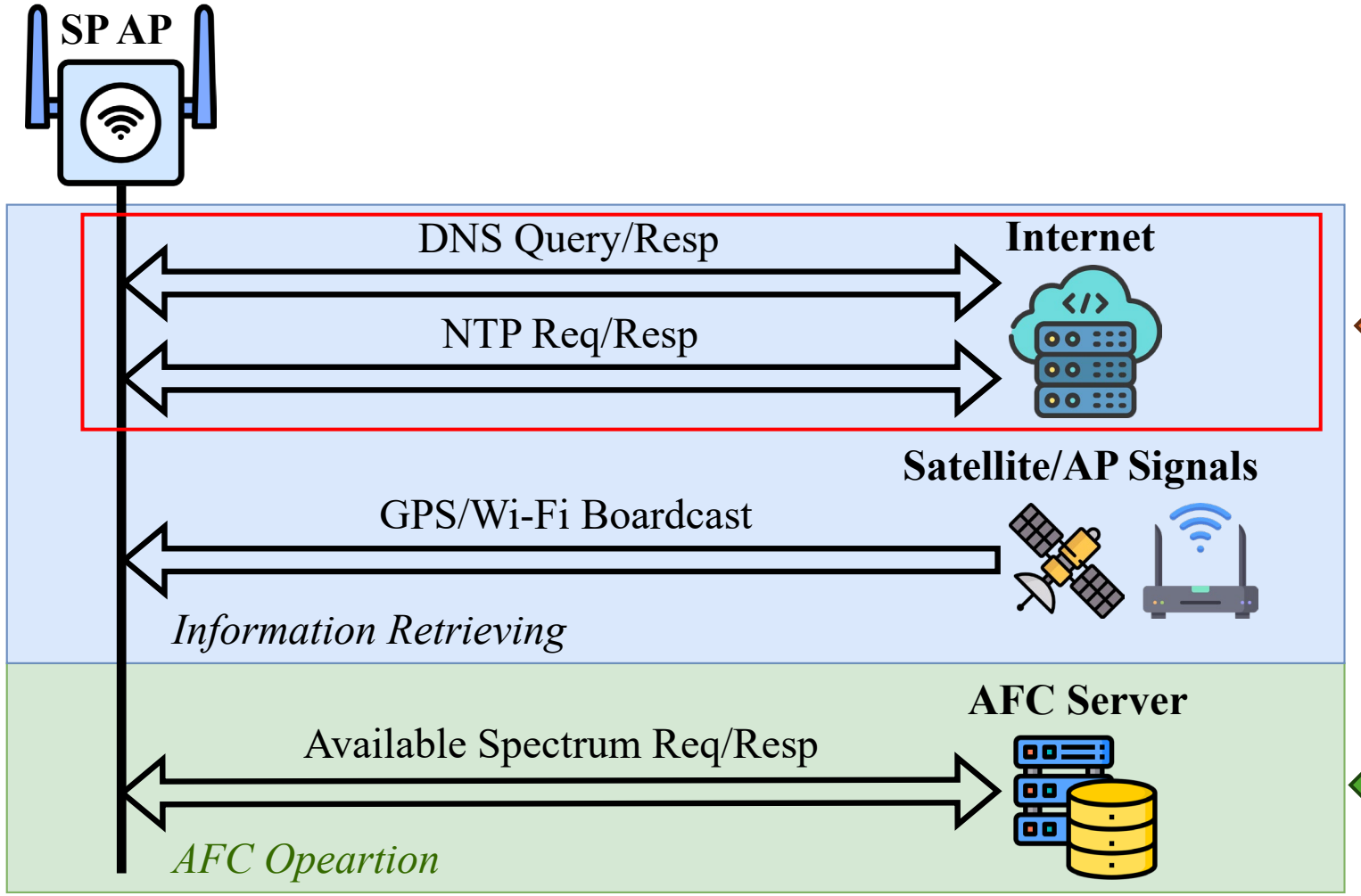
Can an attacker still attack the system, controlling allocated frequency & power (to over/under allocate), even ***without physical access to the AP****?*

AFC Interactions and Attack Surface



Protected by TLS

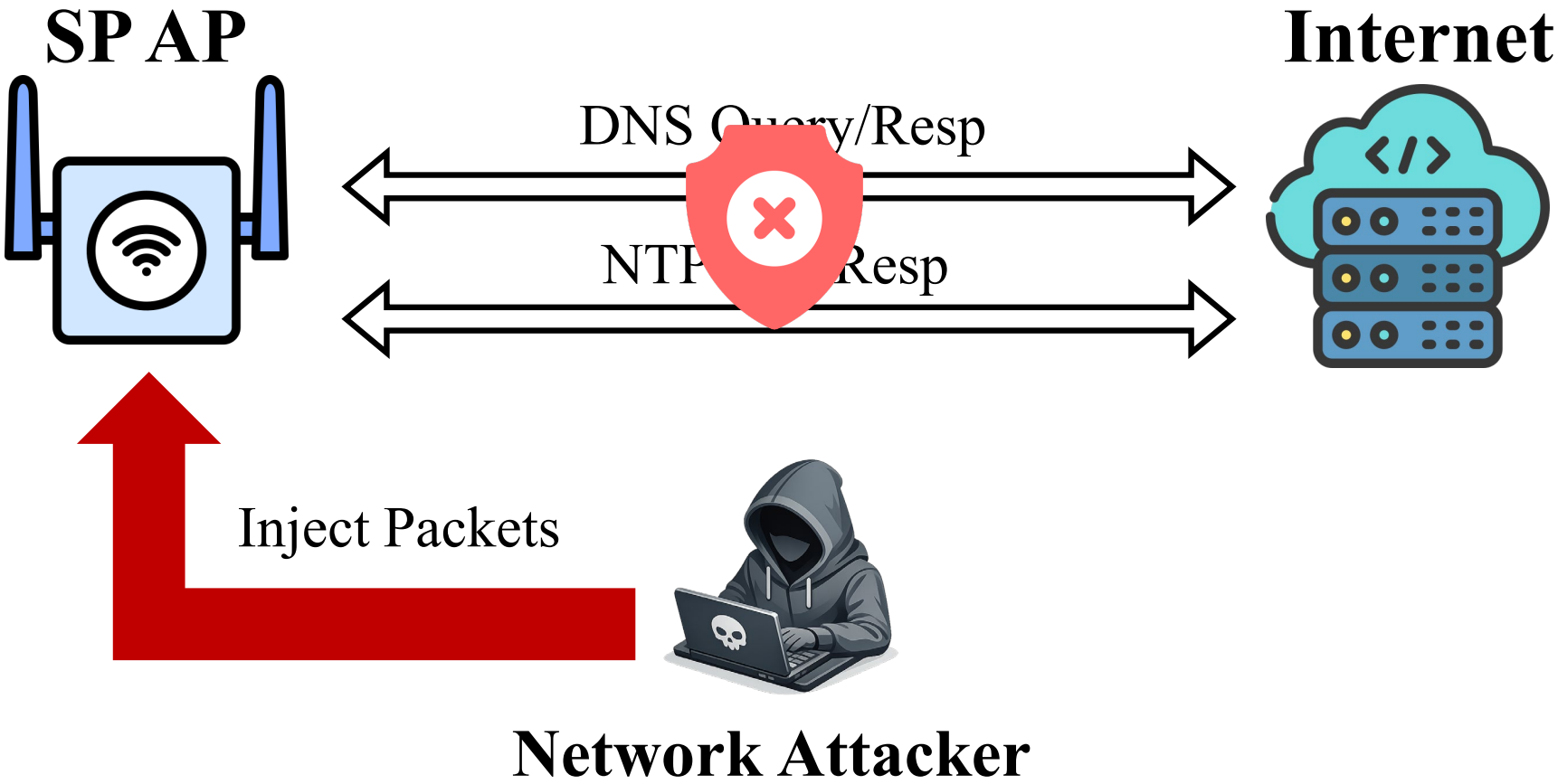
AFC Interactions and Attack Surface



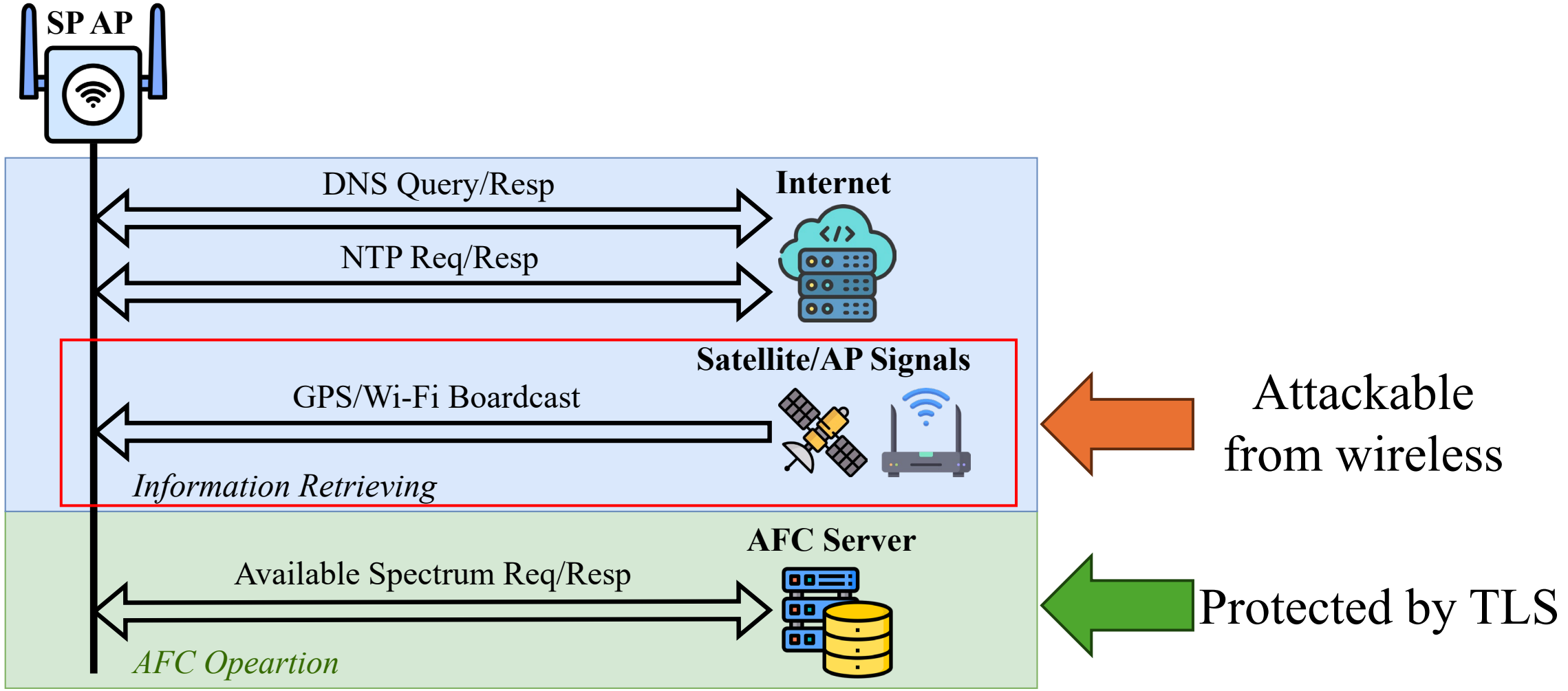
Attackable from network

Protected by TLS

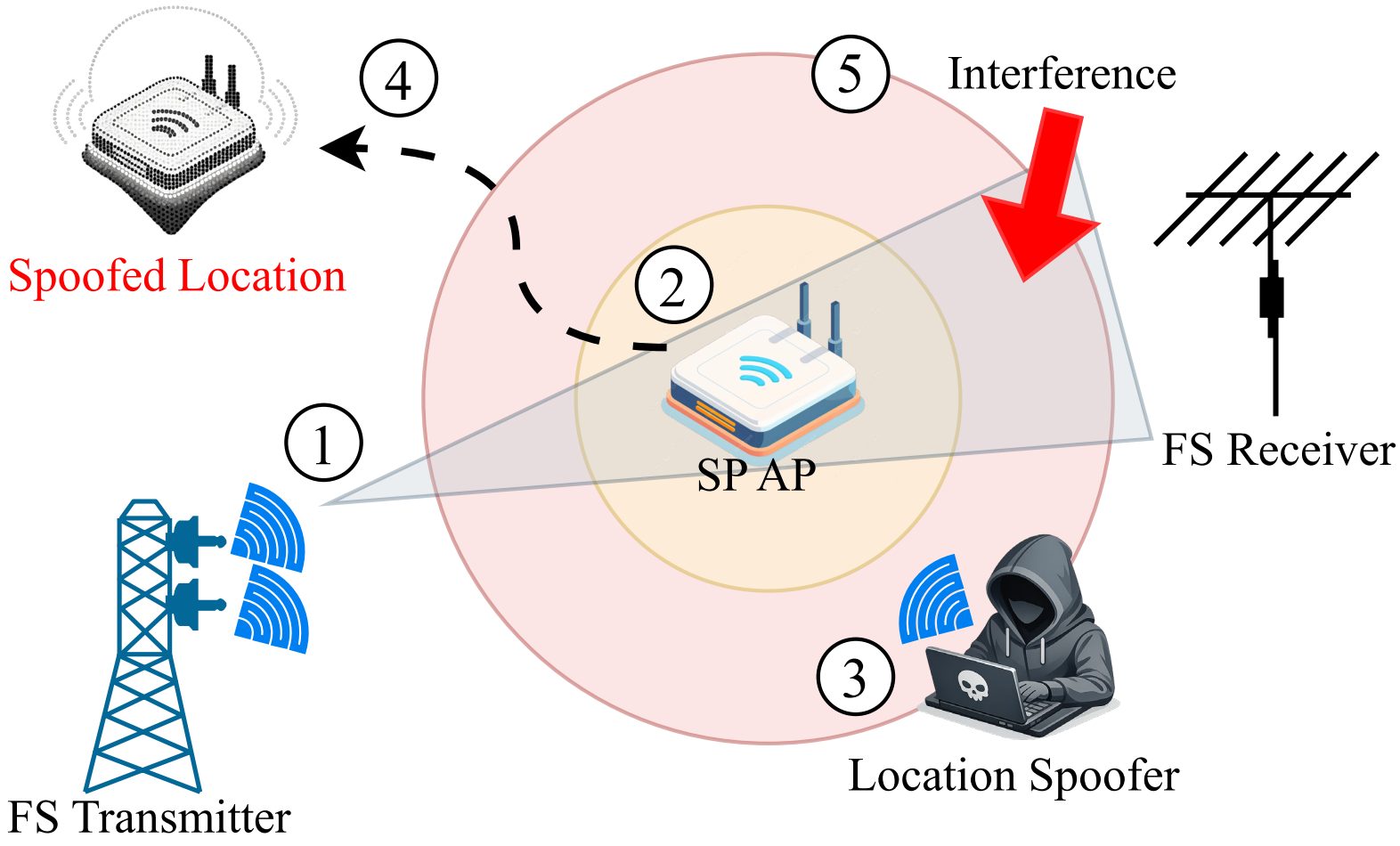
DNS and NTP Attacks



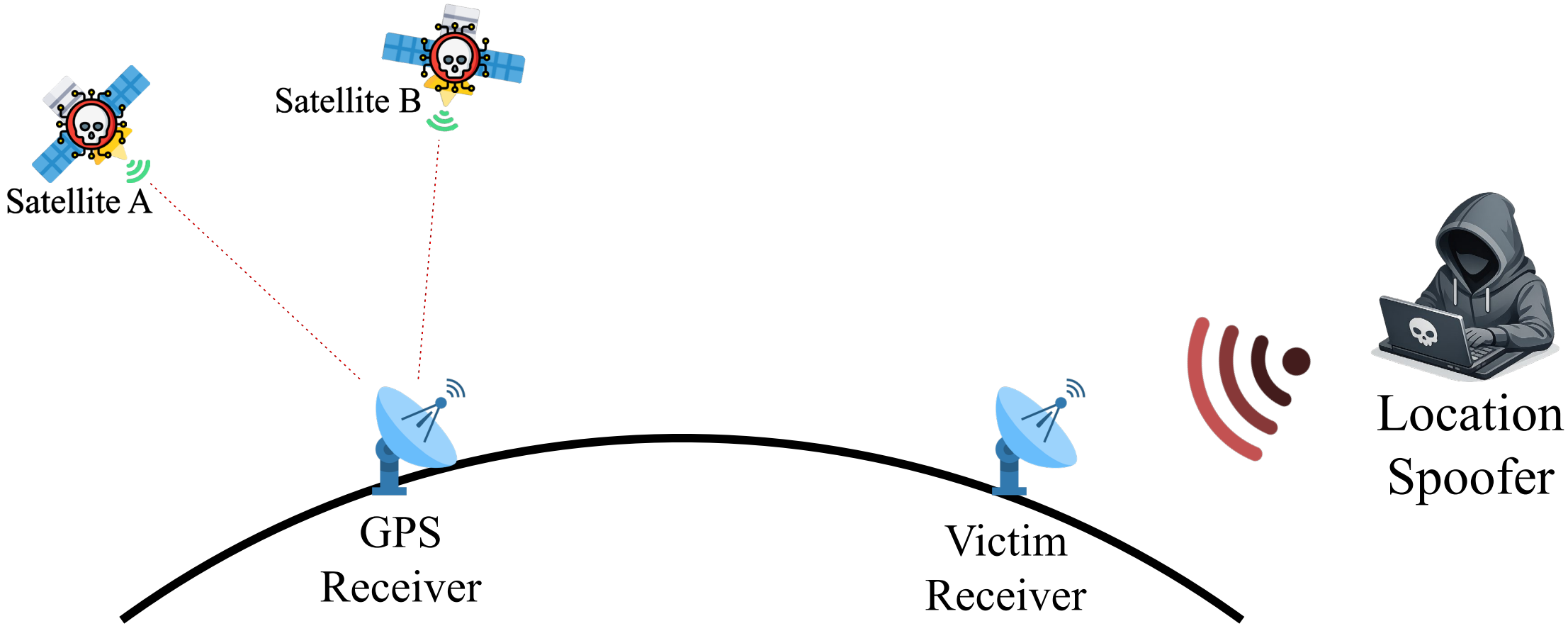
AFC Interactions and Attack Surface



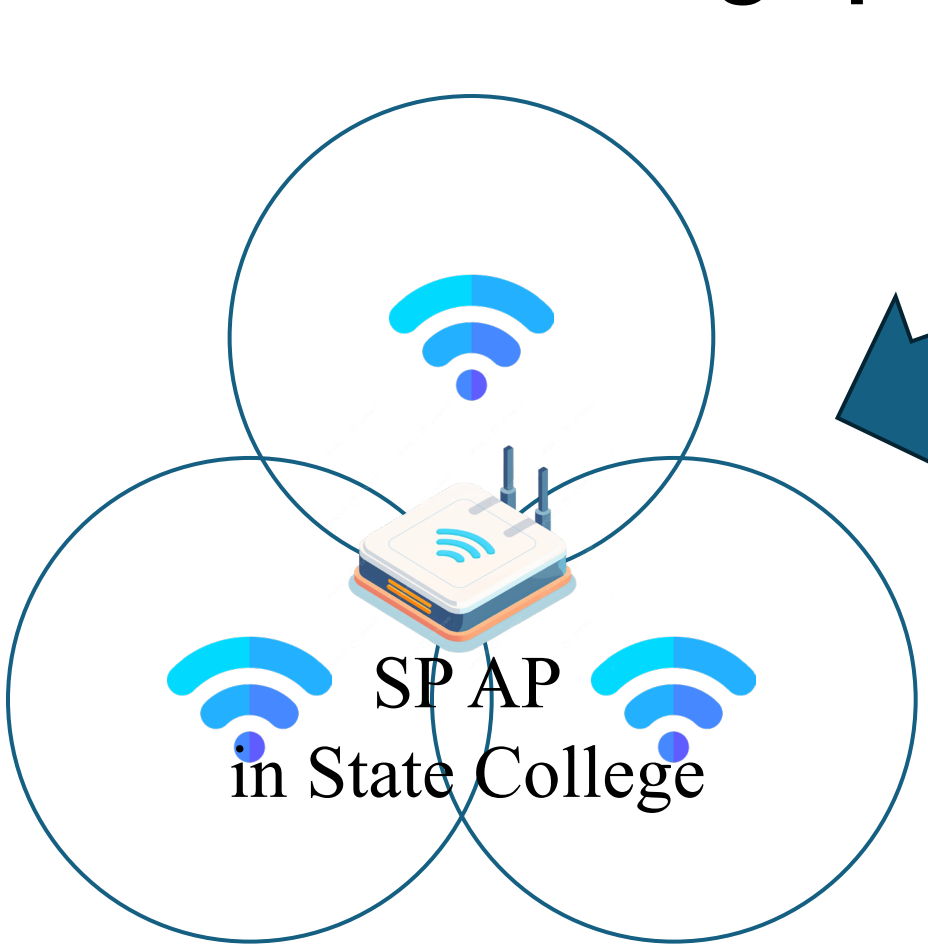
Location Spoofing Attacks against AFC Systems



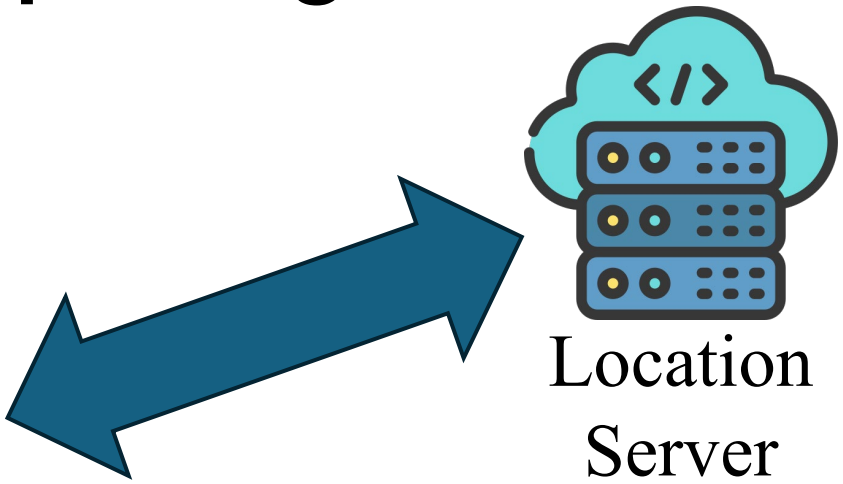
Overview of GPS Spoofing



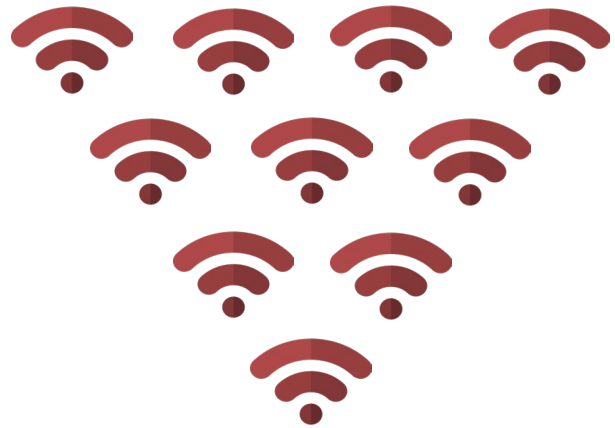
Wi-Fi Positioning Spoofing



SP AP
in State College



Location
Server



APs in New York City retrieved from public database

Location Spoofer

Summary of Attacks

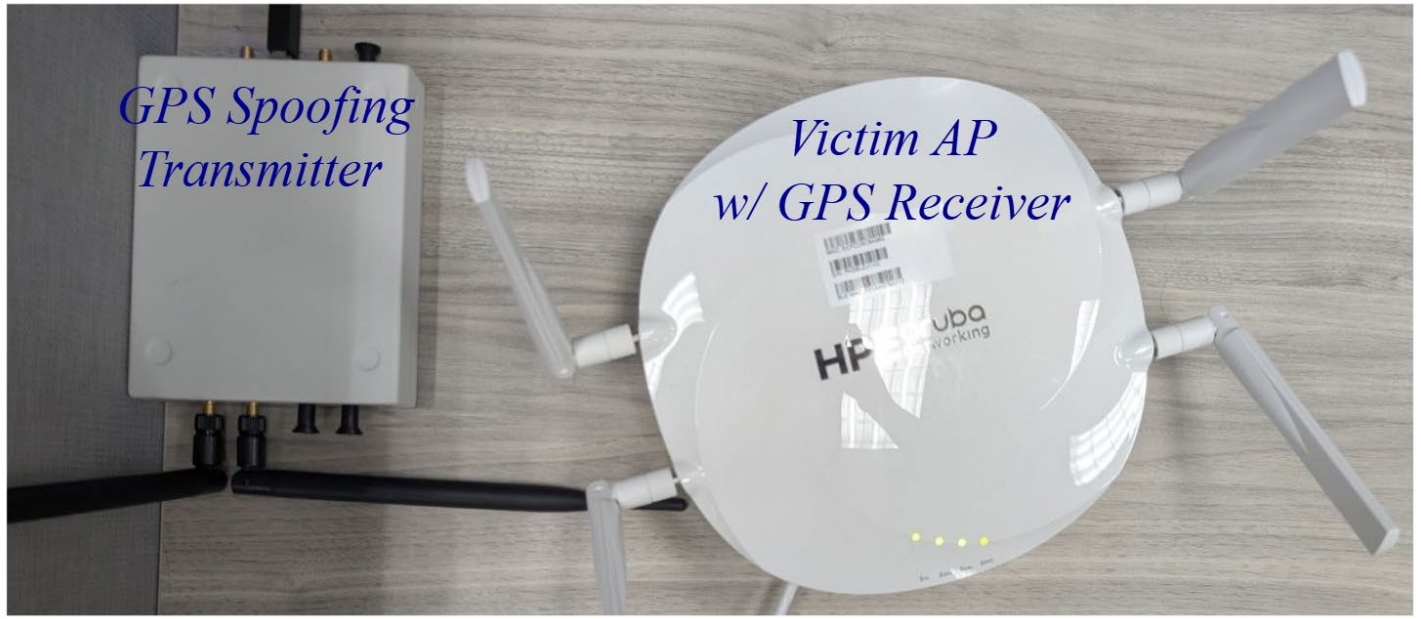
6 attacks on AP, 1 attack on AFC server

Device	AFC Vendor	Localization Type	Plaintext DNS	Plaintext NTP	A1	A2	A3	A4	A5	A6
Aruba AP-634	Federated Wireless	GPS	Yes	Yes	●	●	●	●	●	●
RUCKUS T670	CommScope	GPS	Yes	No	●	●	●	○	●	○
U7 Pro Outdoor	Qualcomm	Wi-Fi	Yes	Yes	●	●	○	●	●	○
ASUS GS-BE18000	Wi-Fi Alliance	Wi-Fi	Yes	Yes	●	●	○	●	●	○

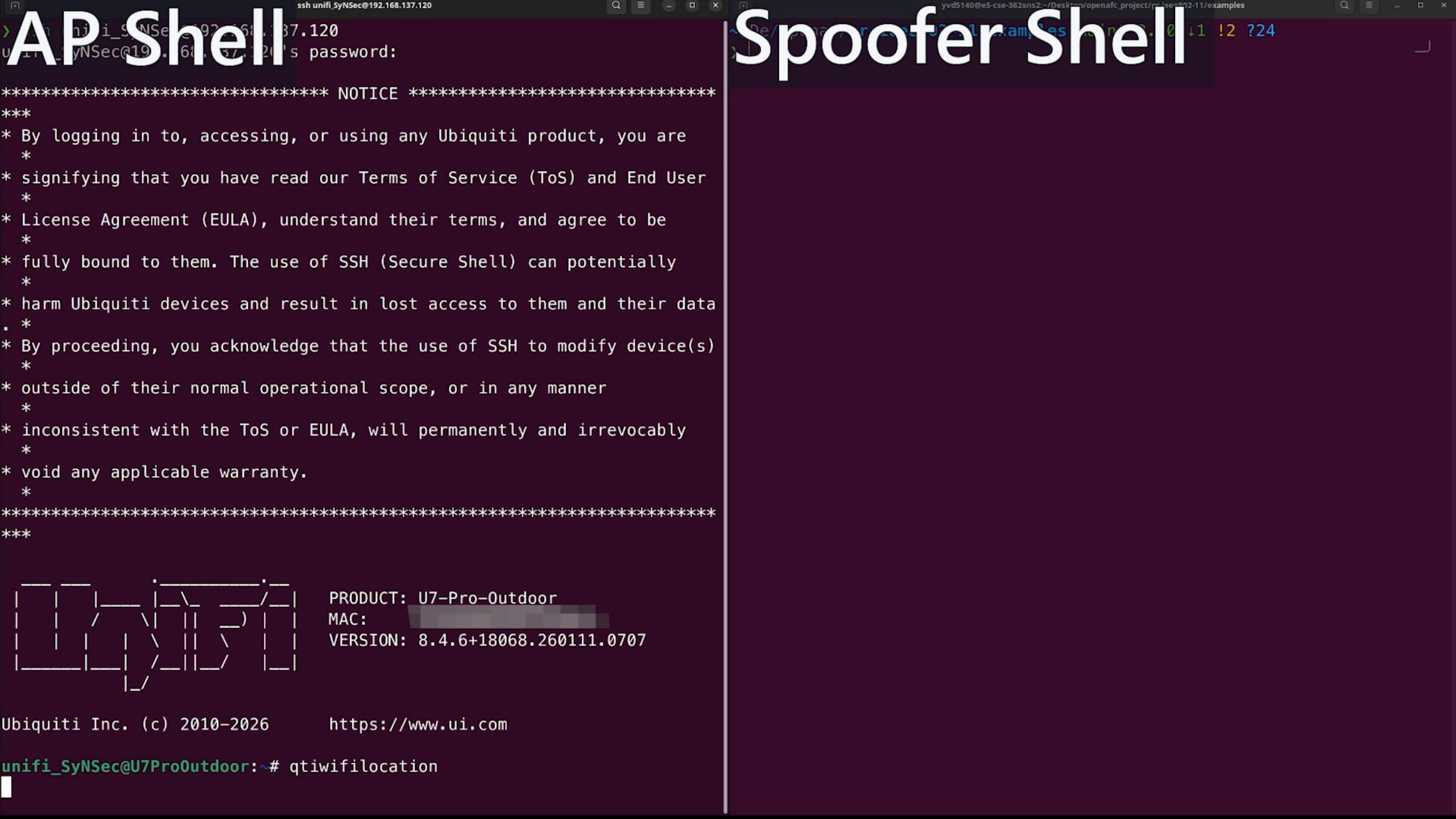
●: Attack applies to the device ○: Attack does not apply to the device

Experiment Setup

- **Transmitter:**
  - USRP B210
- **Software:**
  - GPS-SDR-SIM (GPS)
  - gr-802-11 (Wi-Fi)



Demo: Wi-Fi Location Spoofing on U7 Pro Outdoor


AP Shell
Spoofer Shell
ssh unifi_SyNSec@192.168.137.120
password:
********** NOTICE **********
* By logging in to, accessing, or using any Ubiquiti product, you are
* signifying that you have read our Terms of Service (ToS) and End User
* License Agreement (EULA), understand their terms, and agree to be
* fully bound to them. The use of SSH (Secure Shell) can potentially
* harm Ubiquiti devices and result in lost access to them and their data
* By proceeding, you acknowledge that the use of SSH to modify device(s)
* outside of their normal operational scope, or in any manner
* inconsistent with the ToS or EULA, will permanently and irrevocably
* void any applicable warranty.
PRODUCT: U7-Pro-Outdoor
MAC:
VERSION: 8.4.6+18068.260111.0707
Ubiquiti Inc. (c) 2010-2026
https://www.ui.com
unifi_SyNSec@U7ProOutdoor:~# qtiwifilocation

Interference Attack (A1)

- ❑ Generate the spoofing signal to a rural area
- ❑ The AP send the request with the spoofed coordinate to the AFC server
- ❑ The server reply with **all channels available with maximum allowed power**

```
Max EIRP of AFC channel
20MHz channel       1    5    9   13   17   21   25   29   33   37   41   45   49   53   57   61   65   69   73   77   81
Max Eirp         36.0 36.0 36.0 36.0 36.0 36.0 36.0 36.0 36.0 36.0 36.0 36.0 36.0 36.0 36.0 36.0 36.0 36.0 36.0 36.0 36.0
20MHz channel      85   89   93  117  121  125  129  133  137  141  145  149  153  157  161  165  169  173  177  181
Max Eirp         36.0 36.0 36.0 36.0 36.0 36.0 36.0 36.0 36.0 36.0 36.0 36.0 36.0 36.0 36.0 36.0 36.0 36.0 36.0
40MHz channel       1    9   17   25   33   41   49   57   65   73   81   89  121  129  137  145  153  161  169  177
Max Eirp         36.0 36.0 36.0 36.0 36.0 36.0 36.0 36.0 36.0 36.0 36.0 36.0 36.0 36.0 36.0 36.0 36.0 36.0 36.0
80MHz channel       1   17   33   49   65   81  129  145  161
Max Eirp         36.0 36.0 36.0 36.0 36.0 36.0 36.0 36.0 36.0
160MHz channel      1   33   65  129
Max Eirp         36.0 36.0 36.0 36.0
320MHz_1 channel    1
Max Eirp         36.0
320MHz_1 channel   33
Max Eirp         36.0
```

```
Max EIRP of AFC channel
20MHz channel       1    5
Max Eirp         36.0 36.0
```

Denial-of-Service Attacks (A2-A5)

Impact: No allowed channels in response, the AP cannot transmit in 6 GHz bands.

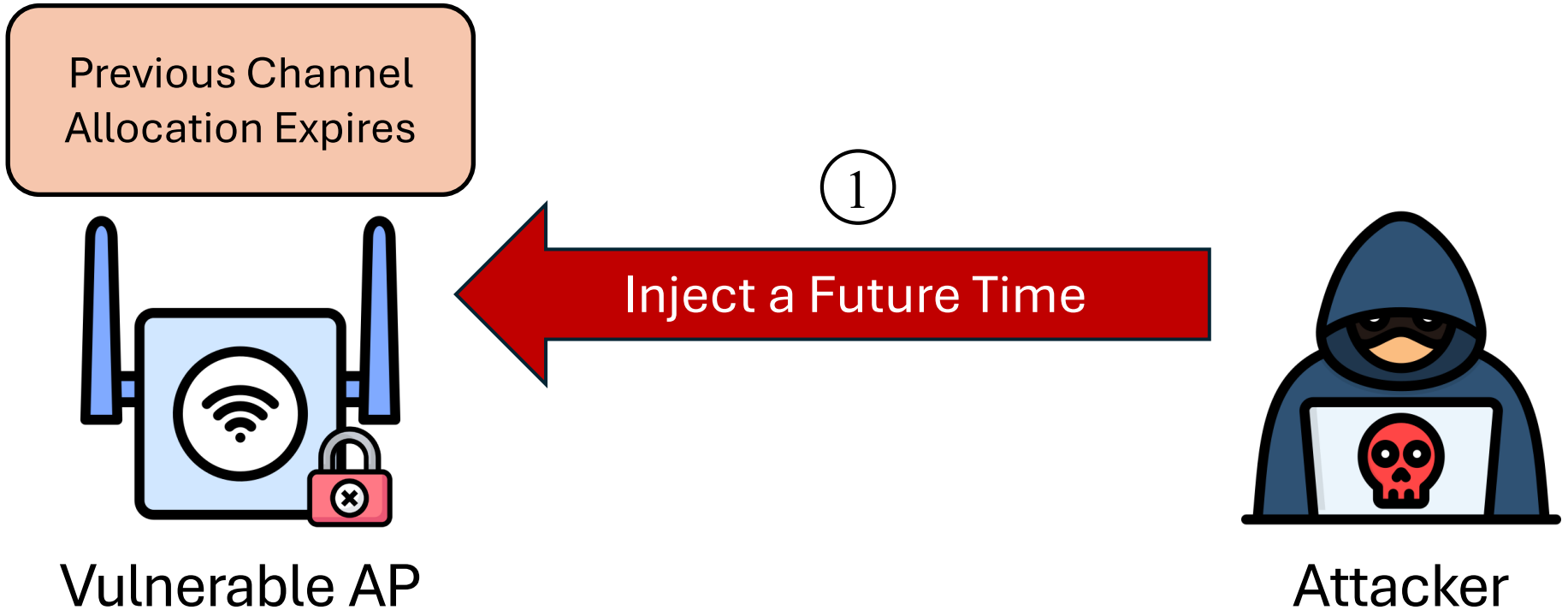
A2: Spoof AP to an invalid location, e.g., a foreign country

A3: Send the GPS signal using invalid time

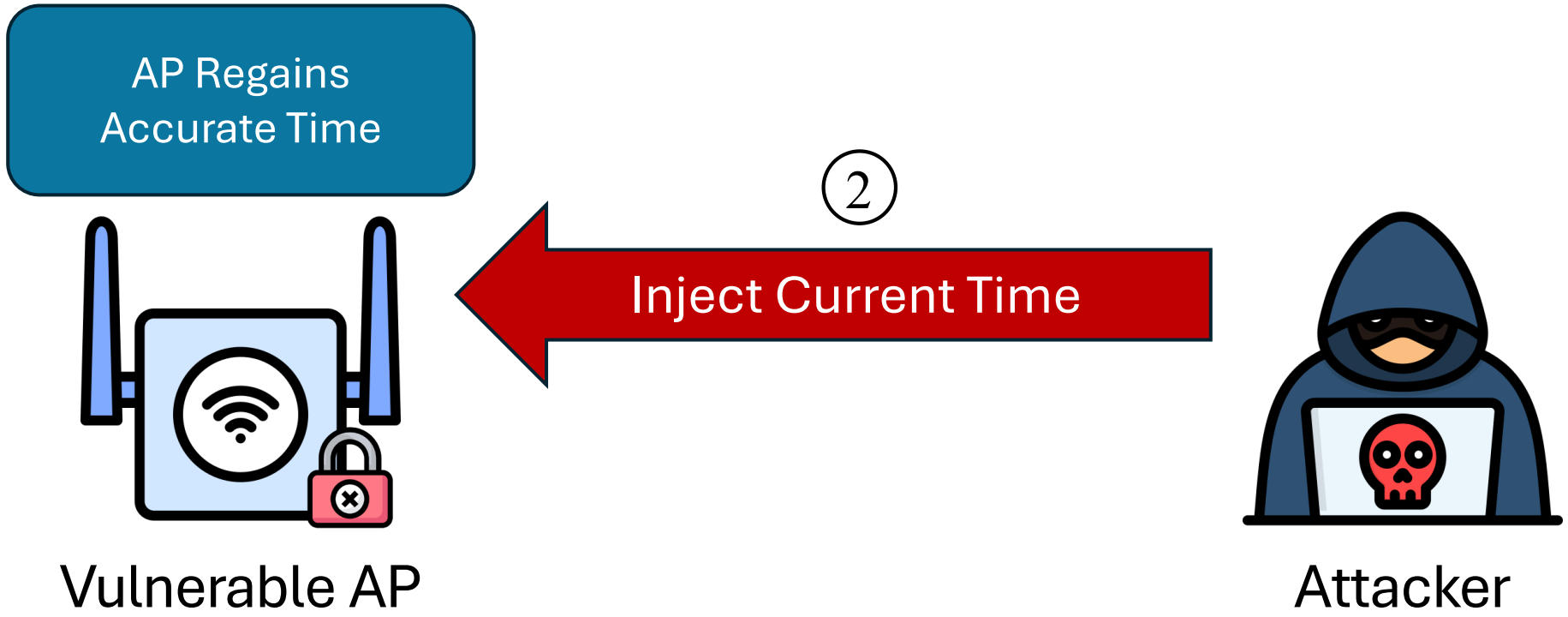
A4, A5: DoS by NTP and DNS Spoofing

```
Received afc channels
---------------------
PHY Type                Allowed Channels
--------                ----------------
6GHz                    None
6GHz 40MHz              None
6GHz 80MHz              None
6GHz 160MHz             None
6GHz 80+80MHz           None
6GHz 320MHz_1           None
6GHz 320MHz_2           None
Present time            2025-06-20 11:36:04
Expiry time             None
Country code            None
AFC channel expired     Yes
AFC channel required    Yes
```

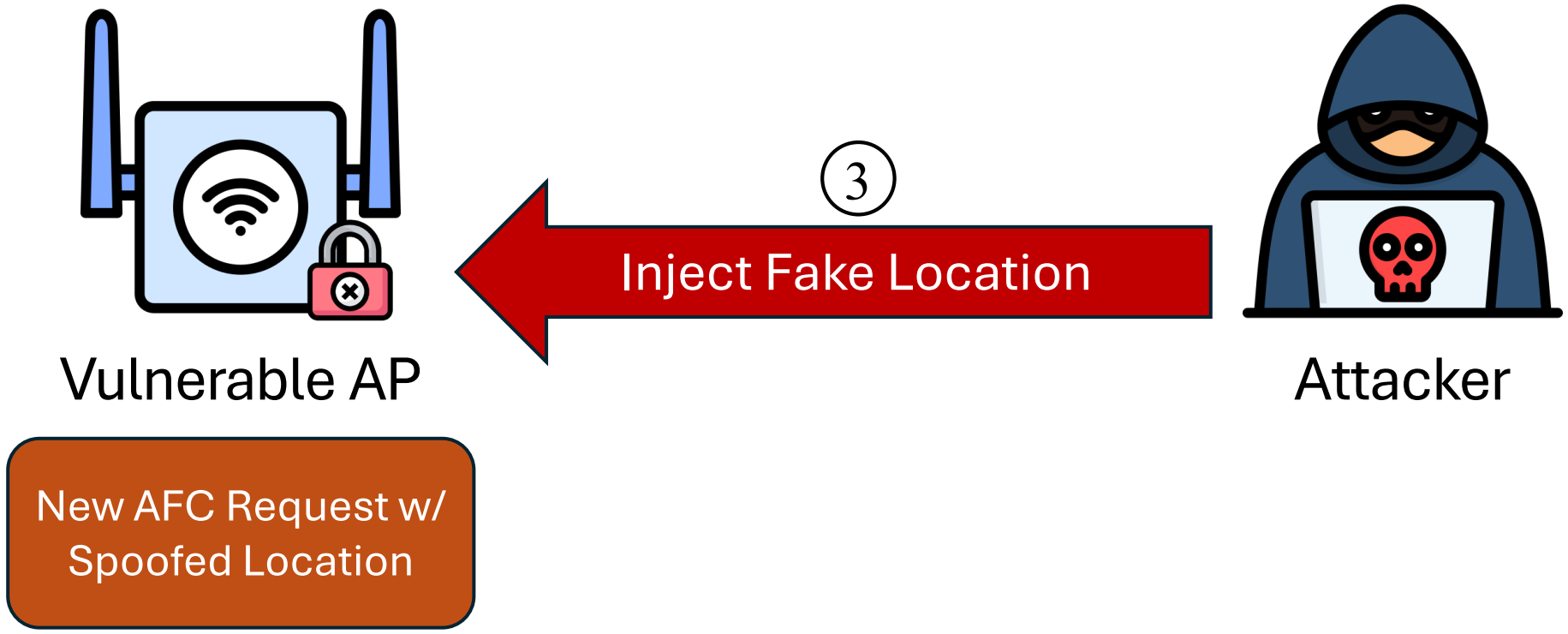
Force Location Update Attack (A6)



Force Location Update Attack (A6)



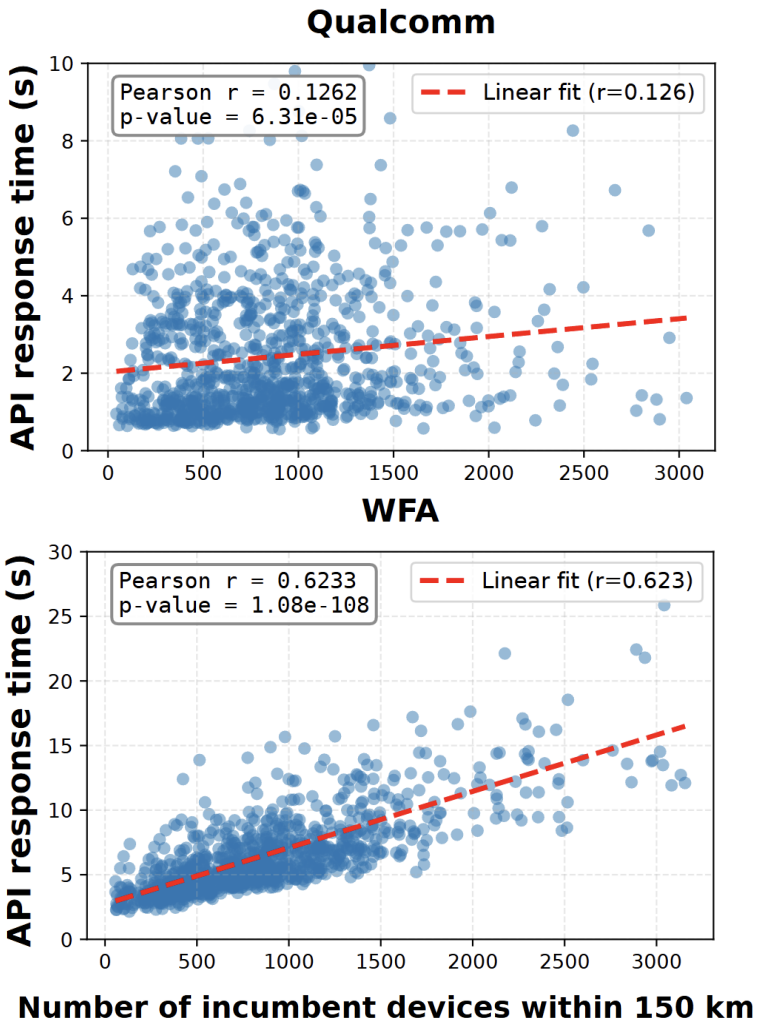
Force Location Update Attack (A6)



Potential Resource Exhaustion on AFC Servers

- ❑ AFC server may also be affected from the manipulated location

- ❑ The **API response time** is correlated with the **number of incumbent devices**
  - Tested on OpenAFC and 2 commercial AFC servers (Qualcomm, Wi-Fi Alliance)



Defenses against Location Spoofing Attacks

❑ Geofencing:

- Pre-define a small possible operation area and stop transmission if outside
- Recommended by HPE Aruba

❑ Fusion of Multiple Location Sources

- Use multiple location sources including network-based location, GNSS and WLAN localization services

❑ Implementation of Detection Mechanisms

- Physical-level spoof signal detection and software-level location tracking

Conclusion and Key Takeaways

- The security of the AFC system is critically dependent on the integrity of its inputs, especially its geographic location
- This trust is misplaced, as demonstrated by practical, low-cost spoofing attacks that can cause interference or denial-of-service
- Defenses against location spoofing should be considered to mitigate these attacks

Thank you!

Yilu Dong
Ph.D. Candidate at Penn State University
Email: yiludong@psu.edu
Website: yilud.me