USENIX

THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

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

Yilu Dong and Tianchang Yang, *The Pennsylvania State University;*
Arupjyoti Bhuyan, *Idaho National Laboratory;*
Syed Rafiul Hussain, *The Pennsylvania State University*

https://www.usenix.org/conference/nsdi26/presentation/dong

This paper is included in the Proceedings of the 23rd USENIX Symposium on Networked Systems Design and Implementation.

May 4–6, 2026 • Renton, WA, USA

ISBN 978-1-939133-54-0

Open access to the Proceedings of the 23rd USENIX Symposium on Networked Systems Design and Implementation is sponsored by

جامعة الملك عبدالله للعلوم والتقنية
King Abdullah University of Science and Technology

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*

Abstract

The 6 GHz band, traditionally reserved for mission-critical incumbent systems such as public safety communications, utility infrastructure, and fixed satellite services, has recently been opened for Wi-Fi devices. This expansion introduces a critical coexistence challenge of ensuring that unlicensed Wi-Fi Access Points (APs) do not interfere with incumbent operations. To manage this risk, regulators mandated the use of Automated Frequency Coordination (AFC) systems that assign spectrum access to Wi-Fi APs based on their locations. In this work, we present the first systematic security analysis of AFC systems. In particular, we analyze the trust assumptions of AFC systems and uncover design lapses and deployment mishaps in this model. Our analysis reveals that the AFC's dependence on unauthenticated data sources, including GNSS/GPS and Wi-Fi-based localization (for location), DNS (for service discovery), and NTP (for time synchronization), creates practical off-path attack vectors that allow adversaries to manipulate control-plane parameters without breaking cryptographic protections between APs and AFC servers. For example, using inexpensive, off-the-shelf software-defined radios, an off-path adversary can spoof the GPS signals received by an AP, falsifying its reported location to either disable 6 GHz transmissions or cause harmful interference with incumbent services. We validate these vectors empirically on commercial APs from four major vendors and evaluate four commercial and one open-source AFC servers to measure real-world impact. We also propose potential mitigations and analyze the trade-offs between usability and security to formulate our recommendations to harden AFC deployments and 6 GHz APs.

1 Introduction

With the rapid growth of Wi-Fi devices, the existing 2.4 GHz and 5 GHz bands have become increasingly congested, leading to interference, degraded performance, and limited throughput. To address these limitations and meet the growing demands of modern wireless applications, the Federal Communications Commission (FCC) opened the 6 GHz spectrum (ranging from 5.925 GHz to 7.125 GHz) for unlicensed use in 2020 [25]. Wi-Fi devices based on 802.11ax (Wi-Fi 6E) [39] and 802.11be (Wi-Fi 7) [40] are authorized to operate in this spectrum. However, these newly available bands overlap with frequencies already used by incumbent licensed devices, many of which support mission-critical infrastructure. These systems include fixed microwave links for cellular backhaul, emergency services (e.g., police, fire, and medical communication networks), and utility telemetry for smart grids. Uncoordinated transmissions from unlicensed Wi-Fi Access Points (APs) operating in the same spectrum could, however, cause harmful interference, potentially disrupting essential services and leading to severe consequences [32].

To enable safe coexistence of incumbent services and unlicensed Wi-Fi devices in the 6 GHz band, the FCC mandates the use of the Automated Frequency Coordination (AFC) system for outdoor, standard-power APs. Similar to the Citizens Broadband Radio Service (CBRS) [7], AFC manages spectrum access to prevent interference. Unlike CBRS, which is hindered by high deployment costs and operational complexity due to its mandate on manual complex setup and continuous server check-in that results in limited consumer adoption, AFC adopts a simpler, offline trust model. It removes the need for special sensing hardware, eliminates manual configuration, and loosens the check-in requirement to a simple 24-hour spectrum lease. While this increased usability facilitates mass deployment in Wi-Fi APs, the associated loose deployment model and implicit trust assumptions introduce significant security risks. Although both commercial APs and AFC systems must be FCC-certified and are expected to operate according to specification, the AFC architecture fundamentally assumes that the location reported by an AP is trustworthy and the AP is operating in a non-hostile network. However, treating these inputs as a root of trust requires strong authentication and integrity protections. A lack of such safeguards can violate these trust assumptions, ultimately undermining the security posture of the entire AFC system. For example, even when

an AP functions correctly and is not physically or remotely compromised, if its externally sourced inputs and discovered services are unauthenticated, they can be manipulated by an external network adversary, thereby influencing frequency authorization decisions and potentially violating interference protections. While existing studies [14, 36] primarily aim to improve the performance and operational capabilities of spectrum-sharing systems, none of them analyze the security and potential risks of these designs.

In this paper, we perform the first systematic study of the trust model underpinning AFC systems, uncover fundamental design lapses and deployment mishaps in this model, and evaluate the security implications this fundamental gap creates for AFC devices and services. Building on our prior workshop paper [22], which demonstrated GPS spoofing on a single AP, this work significantly expands the scope to: **(1)** systematically identify gaps in the security requirements of current technical specifications and regulations, and perform empirical and experimental study of these risks by formulating attack classes that exploit those gaps; **(2)** measure the behavior of commercial Standard Power APs to confirm the presence of vulnerabilities; **(3)** demonstrate end-to-end exploits; and **(4)** further examine open-source and commercial AFC deployments to quantify the security impacts.

Our analysis reveals that AFC's removal of manual setup and continuous validation shifts trust toward critical inputs and discovery services that are often unauthenticated in deployed devices, most prominently GNSS/GPS or nearby Wi-Fi networks (for location), DNS (for service discovery), and NTP (for time). These out-of-band dependencies create practical off-path attack vectors, allowing an off-path adversary to spoof wireless signals, poison DNS responses, or manipulate NTP, causing an AP to report a false location/time, be redirected to attacker-controlled endpoints, or prematurely expire/force AFC leases. Such attacks lead to incorrect frequency/power assignments (which can cause harmful interference to incumbents) and denial-of-service for 6 GHz clients when APs are prevented from receiving valid frequency allocations. Moreover, our investigation uncovers that prohibitively high server-side computation costs induced by attacker-driven bursts of legitimate-looking requests (e.g., forced re-queries) can saturate AFC resources and may lead to wide-area service disruptions, induce incorrect spectrum allocations, or prevent APs from obtaining any 6 GHz channels.

In response to the identified threats, we propose a set of mitigations, including geofencing, the fusion of multiple location sources, and detection mechanisms, to improve the system's robustness. We analyze the trade-offs between usability and security to formulate our recommendations. Additionally, we evaluate potential solutions in consultation with vendors to determine the most cost-effective strategies, specifically recommending the deployment of geofencing.

In summary, we make the following key contributions:

- A systematic characterization and analysis of end-to-end, practical off-path attacks that exploit unauthenticated AFC dependencies and their impact on allocation correctness.
- An empirical study of commercial off-the-shelf 6 GHz APs demonstrating real-world vulnerabilities that enable attacker-controlled allocations, which could lead to harmful interference, elevated power use, or denial-of-service.
- A controlled server-side evaluation that quantifies AFC computation cost and demonstrates a plausible resource-exhaustion attack surface.
- Concrete mitigations and design recommendations to harden AFC deployments and 6 GHz APs.

2 Background

Fixed Service (FS) Link. Fixed Service (FS) links refer to point-to-point or point-to-multipoint wireless communication systems deployed in fixed locations [9]. These links support critical national communication infrastructure, supporting high-capacity data transmission for applications such as Wireless Internet Service Provider (WISP) backhaul, mobile network backhaul (e.g., connecting remote 5G base stations for cellular operators), public safety communications (e.g., FirstNet, a nationwide dedicated broadband network providing priority and preemption for police, fire, and EMS), and telemetry for utilities and critical infrastructure (e.g., wireless sensor networks in smart grids). In the United States and many other countries, FS links are licensed to operate in the 6 GHz spectrum. As these systems were already operating in the band before the introduction of unlicensed Wi-Fi use, they are referred to as *incumbent* users of the spectrum.

Standard Power Access Points. Standard Power (SP) Access Points (APs), introduced with Wi-Fi 6E, are designed to operate in the 6 GHz spectrum and support both indoor and outdoor deployments. These APs transmit at higher power levels compared to low-power indoor APs (Maximum Equivalent Isotropically Radiated Power (EIRP) at 36 dBm), enabling extended coverage and the ability to serve more clients with a stronger and more reliable Wi-Fi signal. However, this increased transmission power also raises the risk of causing interference to incumbent systems (e.g., FS links) operating in the same band. To address this risk, the FCC requires all Standard Power APs to coordinate with an AFC system before operating on the 6 GHz band. While prior work has evaluated the passive interference risk from Wi-Fi 6E deployments [20], it has not considered the possibility of active attacks where an adversary deliberately manipulates the AP's behavior to cause harmful interference. In this work, we focus exclusively on SP APs and use the term AP to refer to them for simplicity.

Automated Frequency Coordination (AFC) System. The Automated Frequency Coordination (AFC) system is a cloud-based service designed to facilitate safe coexistence between unlicensed Wi-Fi devices and licensed incumbent systems in

the 6 GHz spectrum. Its primary role is to determine which channels an AP can use, and at what power levels, to avoid causing harmful interference to incumbent users such as FS links. A properly designed AFC system must ensure the interference-to-noise ratio (I/N) is less than -6 dB for all protected devices.

Figure 1 illustrates the overall architecture of the AFC system. A Standard Power AP initiates the channel authorization process by sending an *availableSpectrumInquiryRequest* message to an AFC provider. This message includes AP's geographic location (typically obtained via GPS), device parameters, and other required metadata. Upon receiving the request, the AFC server queries databases maintained by the National Regulatory Authority (NRA) to retrieve information about protected incumbent systems in the area. It then applies standardized propagation models to calculate the maximum permissible transmission power across each 6 GHz channel. The server returns an *availableSpectrumInquiryResponse* message containing the approved channel and power combinations. An example of *availableSpectrumInquiryRequest* (Listing 5) and *availableSpectrumInquiryResponse* (Listing 6) messages can be found in Appendix A. The AP must comply with this configuration and may only transmit on channels explicitly authorized by the AFC.

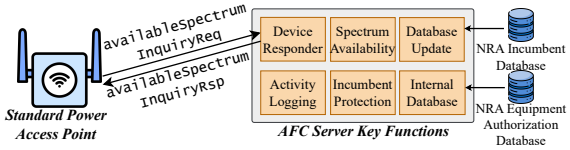

Figure 1: AFC System Architecture

3 Threat Model and Security Requirements

Although AFC channel allocation is logically performed through a single *availableSpectrumInquiryRequest* and *availableSpectrumInquiryResponse* exchange, the correct and robust operation of a Standard Power (SP) 6 GHz Wi-Fi AP depends on a sequence of external communications, as illustrated in Figure 2. To systematically characterize the associated risks, we analyze the security of this end-to-end communication workflow and identify the resulting attack surfaces.

3.1 AFC Design and Trust Assumptions

The AFC system architecture represents a distinct evolution in spectrum management, prioritizing scalability and automation to accommodate the mass deployment of unlicensed Wi-Fi devices. Previously, the Citizens Broadband Radio Service (CBRS) [7], a shared spectrum framework operating in the 3.5 GHz band, relied on Certified Professional Installers [62] for installation parameter validation and Environmental Sensing Capability (ESC) networks for incumbent detection [46]. It also mandates strict real-time control, requiring devices to communicate continuously with the Spectrum Access Server

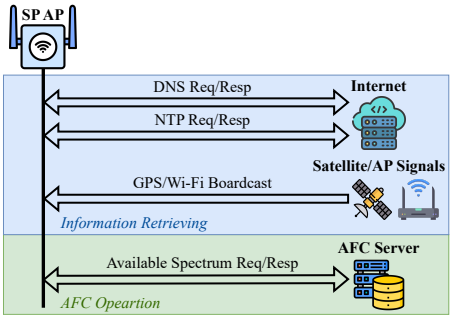

Figure 2: Interactions Required for Correct Operation of AP

(SAS) and adjust parameters within 60 seconds [8]. Although these measures effectively protect incumbents (e.g., naval radar), the reliance on hardware and human-in-the-loop verification limits scalability. Consequently, consumer adoption remains low, resulting in inefficient spectrum usage [52].

In contrast, the AFC system eliminates these external verification layers and targets mass-market Wi-Fi. Adding trusted hardware-backed solutions, e.g., tamper-resistant geographic positioning modules or third-party independent validation mechanisms such as ESCs or installer certification, increases bill-of-material costs and slows time-to-market in a highly price-sensitive ecosystem. Hence, AFC systems rely entirely on the AP to self-report its geographic location and device parameters to a centralized cloud server. This design significantly lowers deployment barriers (e.g., zero-touch provisioning) and increases flexibility, but introduces a critical assumption: the AFC server must implicitly trust that the AP's inputs are accurate and untampered with. In the absence of hardware-based solutions or external verification, the integrity of spectrum coordination depends solely on the correctness of AP-reported parameters.

This architecture embeds several core trust assumptions: ❶ The AP accurately determines and reports its geographic location. ❷ Reported device parameters (e.g., antenna height, power class) reflect the actual physical configuration. ❸ The AP software interacting with the AFC server has not been modified to manipulate inputs. ❹ The communication channel between the AP and the AFC server preserves authenticity and integrity. To manage the risks inherent in this fully automated, self-reporting architecture, regulators and standards bodies have established a baseline set of compliance-focused security constraints, assuming that certified APs behave benignly.

3.2 AFC Security Requirements

Based on a comprehensive manual analysis of the AFC system requirements (WINNF-TS-1014) [63] and the federal regulation 47 CFR § 15.407(k) [10], we identify the following security requirements that govern the operation of AFC systems as specified by existing standards and regulations:

- **(REQ1)** The communication between the AP and the AFC server must be mutually authenticated, encrypted, and

integrity-protected.

- **(REQ2)** Access to the internal AFC databases, including lists of protected incumbent systems, must be strictly controlled to prevent unauthorized access or modification.
- **(REQ3)** The AFC server must correctly compute and return the permissible frequency and power levels based on the AP's reported parameters, thereby ensuring reliable protection of incumbent services.

These guarantees are typically enforced via Transport Layer Security (TLS) for all AP-to-server communication [60]. Provided the AP functions correctly and its TLS stack remains uncompromised, an attacker cannot eavesdrop on, tamper with, or spoof AFC messages. Therefore, in the following threat analysis in this section, we assume these three requirements are correctly enforced, i.e., the operations in the green region in Figure 2 are all correct and not tampered with. In §7, we further validate these assumptions by experimentally testing commercial AP devices.

3.3 Threat Model

In this work, we consider that the AP is operating unaltered and the three specification requirements detailed in §3.2 are all satisfied. The adversary has no direct control of the AP and cannot compromise its software, firmware, or hardware. The attacker also lacks valid authentication credentials and TLS session keys, and therefore cannot perform an active machine-in-the-middle (MitM) attack on the AP–AFC channel. Under these assumptions, the adversary is limited to *off-path* attacks that influence the external inputs or sensors the AP relies on to obtain AFC authorization (for example, location or timing signals), or that otherwise interfere with the AP's ability to obtain or apply correct frequency and power assignments. The attacker's goal is to cause the AP to request or use incorrect parameters, to provoke denial-of-service for 6 GHz clients, or to induce transmissions that may interfere with incumbent systems or radio observatories, e.g., national radio astronomy observatory (NRAO), protected by the AFC.

4 Attack Surface Analysis

The requirements in §3.2 enforce assumptions ❸ and ❹ in §3.1, namely software integrity and secure AP–AFC communication. However, they do not guarantee assumptions ❶ and ❷, which concern the correctness of AP-reported location and device parameters. Even when the AP–AFC channel is cryptographically protected, the AFC server's core decisions (e.g., allowed frequency and power) depend almost entirely on inputs reported by the AP, including geographic location and device metadata. The protocol- and backend-focused protections specified in §3.2, therefore, rest on the implicit trust assumption that these inputs are correct. This design implies that regulators may have underestimated the capabilities of potential attackers, assuming that external environmental inputs are trustworthy. If an adversary can manipulate the AP's input sources, they can subvert AFC decisions despite the cryptographic protections of the AP–server channel. We characterize this attack surface as *input-manipulation attacks* against the AP's information-retrieval phase (Figure 2). This phase depends on external services that are not, in general, protected end-to-end. Common dependencies include location determination, service resolution, and time synchronization.

Because these attacks manipulate inputs that the AFC implicitly trusts, they bypass the assumption that a secure channel alone guarantees correct behavior. An adversary who controls or falsifies these inputs can induce denial-of-service for 6 GHz clients or cause AP transmissions that violate incumbent protection requirements, without breaking any cryptographic guarantees enforced by existing specifications.

4.1 Lack of Location Data Integrity

Standard Power APs rely on external localization sources to determine the geographic coordinates reported to the AFC server. In practice, this often includes GNSS/GPS, but AFC regulations do not mandate a specific localization mechanism [10]. Regardless of the source, the AFC server implicitly trusts the AP-reported location. This creates a direct attack surface: if the location input can be manipulated, the AFC decision can be subverted.

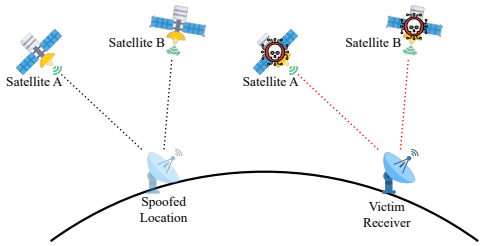

Figure 3: GPS Spoofing Attack

GNSS/GPS Spoofing. Civilian GPS signals are unauthenticated and received at extremely low power (below -100 dBm) [12]. As a result, an attacker can overpower legitimate satellite signals using inexpensive commercial-off-the-shelf hardware, e.g., a Software-Defined Radio (SDR) like the $400 HackRF Pro [30], placed within effective range. Such transmitters range from inexpensive, short-range setups to more capable platforms coupled with directional antennas or remote drone platforms. As illustrated in Figure 3, an attacker can generate GPS signals corresponding to an arbitrary location and transmit them to the victim AP. Upon receiving the spoofed signals, the AP computes and reports the fabricated coordinates to the AFC server. Recent work has demonstrated increasingly practical spoofing techniques that are harder to detect [57], scalable over larger areas [56], and cheaper to deploy [17]. Consequently, GPS spoofing remains a realistic threat to AFC-enabled devices.

Wi-Fi based Location Spoofing. GNSS-based localization requires additional hardware and may increase the cost of Wi-Fi APs. To incorporate AFC in customer-grade products, AP vendors often instead rely on Wi-Fi-based positioning [51]. These products scan for nearby networks, collecting MAC addresses and received signal strength indicators (RSSI) to estimate their position via a location server. According to Wi-Fi standards, APs broadcast beacon frames to facilitate network discovery. However, these frames lack cryptographic authentication. Because the AP cannot verify the origin of these signals, this lack of authenticity enables an attacker to spoof beacon frames that mimic known APs, thereby manipulating the location calculation [31, 58].

Spoofing of Alternative Localization Methods. AFC regulations do not restrict the localization source to GNSS or Wi-Fi [10]. AP vendors may instead rely on network-based positioning [27], cellular base stations [19], or administrator-configured fixed coordinates. These mechanisms are likewise susceptible to spoofing. Network-based localization can be manipulated through a VPN [45], while cellular-based positioning can be influenced by falsified broadcast messages from rogue base stations [54] or machine-in-the-middle relays [38]. Therefore, the vulnerability is not specific to localization methods, but spans the broader architectural assumption that the AP-reported location is trustworthy.

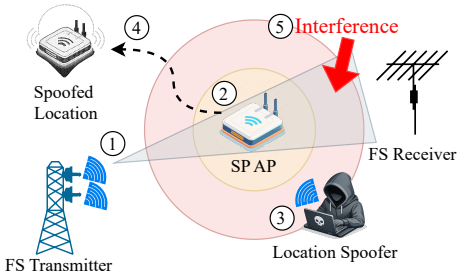

Figure 4: AFC Attack on Fixed Service (FS) Links

Impact on AFC Decisions. Figure 4 illustrates location spoofing's impact on AFC operation. During benign operation, ① an active FS link and ② an AP at its true location coexist without interference (shown as the yellow circle). Under attack, ③ an adversary spoofs the AP to ④ a false location with fewer constraints. By reporting this in its *availableSpectrumInquiryRequest*, the AP obtains a higher permitted transmit power (the red circle), resulting in ⑤ direct interference with the FS receiver. Conversely, spoofing the AP to a restricted area or blocking location acquisition entirely triggers channel denial, causing a denial-of-service for 6 GHz clients.

4.2 Missing Time Integrity

Reliable time is critical for AFC compliance, which mandates daily re-authorization [10]. However, many APs rely on unauthenticated Network Time Protocol (NTP) over plaintext UDP. Attackers can exploit this by spoofing DNS/DHCP responses [13] or injecting packets to redirect APs to malicious timeservers. As shown in prior work [44, 49], manipulating time can force premature lease expiration (causing the AP to stop service), induce persistent clock skews, and disrupt security mechanisms like certificate validation. These network-level attacks pose a realistic threat to AFC integrity without requiring physical access.

4.3 Unauthenticated DNS Data

Domain Name System (DNS) resolution is a ubiquitous but often unauthenticated dependency on which APs rely to locate endpoints, including AFC or NTP servers. If DNS responses can be spoofed or poisoned (e.g., cache poisoning or compromise of a resolver), an off-path attacker can redirect an AP to attacker-controlled infrastructure or to nonexistent addresses, producing either silent misdirection or straightforward denial-of-service [35]. Redirecting DNS to an attacker host can enable further attacks (for example, supplying bogus configuration, malicious update manifests, or attacker-controlled NTP endpoints) and outages. For secured channels (e.g., TLS), defeating protections would additionally require compromised or stolen keys.

4.4 Lack of Integrity of Other Data

In this work, we focus on three pervasive and unprotected dependencies found in the commercial APs we acquired: location, DNS, and NTP. Although these are our primary focus, the underlying input-spoofing methodology applies to any service that lacks robust authentication. For example, network protocols like DHCP can be spoofed to redirect traffic [11], while management interfaces like vendor cloud APIs [23], insecure OTA updates [64], and RADIUS/AAA controllers [28] can be used to inject malicious settings. In addition, spectrum-sensing inputs can be spoofed to force unsafe channel choices [55]. Ultimately, any unauthenticated dependency represents a potential vector for an attack designed to disrupt AFC operations.

5 Detailed Spoofing Methodologies

GPS Spoofing. We implement GPS spoofing using the open-source software GPS-SDR-SIM [24] to synthesize GPS signals for the target coordinates, which are then transmitted via a USRP B210 [5]. Initial naive attempts failed because the generated signals lacked up-to-date ephemeris data and current timestamps [59]. To ensure successful spoofing, we incorporate the latest public Ephemeris data and pre-generate signal samples with a future timestamp (30 seconds ahead). Transmission is delayed until this specified time to ensure the victim AP successfully decodes and accepts the signals. Following a data collection period (e.g., 20–30 minutes for

the HPE Aruba AP), the AP updates its internal location estimate, subsequently including this falsified location in its *availableSpectrumInquiryRequest* to the AFC server.

Wi-Fi Location Spoofing. Successfully spoofing Wi-Fi geolocation entails more than simply broadcasting beacon frames. To ensure validity, the attack must simulate a sufficient number of networks indigenous to the target coordinates; otherwise, the geolocation service may reject the signals as anomalous or inconclusive. To replicate realistic Wi-Fi environments, we query the crowd-sourced database WiGLE [16] to retrieve valid AP configurations for a target location, prioritizing those closest to the coordinates to maximize accuracy. We then employ a modified version of gr-ieee802-11 [15] on a USRP B210 to transmit spoofed beacon frames using the retrieved MAC addresses. When the victim AP detects these signals, it incorporates the spoofed APs into its scan results, causing the location server to return the falsified coordinates.

DNS and NTP Spoofing. To evaluate DNS and NTP attacks deterministically, we establish a machine-in-the-middle (MitM) setup between the target AP and the Internet to manipulate unencrypted traffic. In practice, an off-path attacker could achieve identical outcomes by exploiting race conditions or injecting spoofed packets.

6 Attacks on AP & Impact Analysis

We perform systematic security tests of the attack vectors discussed in §3 on 4 commercial-off-the-shelf (COTS) APs with AFC support, all from different vendors: the HPE Aruba AP-634 [2] (AFC service provided by Federated Wireless), RUCKUS T670 [4] (AFC service provided by CommScope), Ubiquiti UniFi U7 Pro Outdoor [1] (AFC service provided by Qualcomm), and ASUS GS-BE18000 [3] (AFC service provided by Wi-Fi Alliance). Of the tested APs, both Aruba and RUCKUS use a GPS receiver to retrieve their current locations to report to AFC. The Ubiquiti U7 Pro Outdoor and the ASUS GS-BE18000 use nearby Wi-Fi APs to locate themselves. We perform location spoofing by transmitting GPS or Wi-Fi signals with USRP B210 [5]. We modify GPS-SDR-SIM [24] and gr-ieee802-11 [15] to generate the GPS and Wi-Fi signals, respectively. Figure 5 shows a sample experiment setup of GPS spoofing attacks on HPE Aruba AP-634. All the experiments are performed in a controlled environment with no devices other than the tested APs affected.

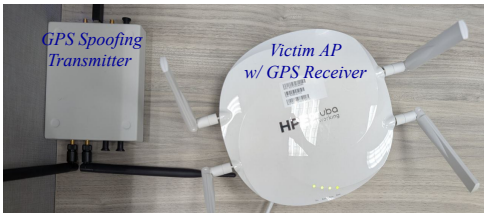

Figure 5: Experiment Setup

6.1 Security Measures in Commercial APs

We verified the following security measures in the tested COTS APs and confirmed that all of them complied with the security requirements discussed in §3.2.

- **(AP-M1)** All the communication between the AP and the AFC server (and management server) is protected by TLS (comply with **REQ1**).
- **(AP-M2)** The firmware of the AP is not publicly available, and the low-level control of the AP is not available to a normal user (comply with **REQ2**).
- **(AP-M3)** The AP correctly followed the list of available frequency and power allocation returned by the AFC server. (comply with **REQ3**).

However, these security measures are not enough to prevent other attack surfaces discussed in §4. We uncovered six distinct attacks (**A1**–**A6**), all of which are previously unexplored in the AFC domain and can be launched by an off-path attacker. Table 1 summarizes which attacks succeeded against each tested AP device. We include representative console outputs from the HPE Aruba AP to demonstrate each attack. Other devices tested showed similar behaviors, and additional results can be found in Appendix B.

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

Table 1: Attacks on Tested Devices

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

6.2 A1: Interference Attacks

Receiving Spoofed Signal. After the AP receives the spoofing signal, it calculates its location and location uncertainty in an elliptical form. As an illustrative example, we generate spoofing signals for the coordinate (30.086965, -101.103761), located in a rural area of Texas. However, the location computed by the Aruba AP is at coordinate (30.087050, -101.103714), 10 meters from the spoofed location. The error is likely introduced by an inaccurate clock in our transmitter. Listing 1 is an example output from the AP console. We observed similar results across all tested APs for other spoofed locations.

```
GPS ELLIPSE Information
-----------------------
Field       Value
-----       -----
latitude    30.087050
longitude   -101.103714
major-axis  18.052600
minor-axis  1.665372
angle       115.498839
time        2025-06-20 04:57:53
```

Listing 1: GPS ELLIPSE Information from Aruba AP

Receiving AFC Channels Available. After the AP calculates its location from spoofed signals, it sends the *availableSpectrumInquiryRequest* to the AFC server and receives

the *availableSpectrumInquiryResponse*. Listing 2 provides a list of received AFC channels from the Aruba AP in the response message, including all available 6 GHz Wi-Fi channels permitted in the United States, valid for 24 hours.

```
Received afc channels
PHY Type              Allowed Channels
6GHz                  1 5 9 13 17 21 25 29 33 37 41 45 49
                      53 57 61 65 69 73 77 81 85 89 93 117
                      121 125 129 133 137 141 145 149 153
                      157 161 165 169 173 177 181
6GHz 40MHz            1 9 17 25 33 41 49 57 65 73 81 89
                      121 129 137 145 153 161 169 177
6GHz 80MHz            1 17 33 49 65 81 129 145 161
6GHz 160MHz           1 33 65 129
6GHz 80+80MHz         None
6GHz 320MHz_1         1
6GHz 320MHz_2         33
Present time          2025-06-20 05:13:13
Expiry time           2025-06-21 05:10:00
Country code          US
AFC channel expired   No
AFC channel required  Yes
```

Listing 2: Received AFC Channels of **A1** from Aruba AP

Power Associated with Channels. Listing 3 provides the channel and the associated transmission power in Equivalent Isotropically Radiated Power (EIRP). In this spoofed location, all the channels are associated with the maximum power allowed in the specification, 36.0 dBm. The AP can select from these channels and start transmission with a power under the specified maximum power limit, causing potential interference to other spectrum users.

6.2.1 Impact of Interference Attacks

We validated the interference attack across all tested APs. Unlike directly transmitting interference signals, this attack leverages the AFC system itself to amplify the impact. By spoofing the AP's location, an attacker can cause the AFC server to authorize higher transmit power and more channels than would normally be permitted. For comparison, a USRP B210-based jammer is limited to sub-6GHz frequencies, transmitting at a maximum of 20 dBm [6] across a 56 MHz bandwidth. In contrast, by using the same USRP for location spoofing, an off-path attacker can force a victim AP to transmit at frequencies up to 6875 MHz on a 320 MHz channel at maximum power (36 dBm), completely overriding the AFC system's location-based power limits. Under these conditions, the AP may use the additional power to cause harmful interference to incumbent systems. If located near a mission-critical FS link, it may interrupt ongoing communication. If deployed near a radio observatory, it may affect sensitive astronomical observations. Furthermore, we observed that all tested APs do not re-contact the AFC server before the lease expires, even if the spoofing signal stops. As a result, a successful attack may persist for up to 24 hours. An attacker can therefore spoof the locations of multiple APs simultaneously, increasing both the number of interference sources and the geographic impact. Because the interference originates from legitimately authorized AP transmissions, detection becomes more challenging. Together, this allows the attacker to amplify interference power, scale the number of affected transmitters, prolong the attack duration, and reduce detectability.

Interference to Incumbent Devices. The primary goal of an AFC system is to protect incumbent services by ensuring the interference-to-noise ratio (I/N) at their receivers remains below -6 dB [60]. Attacks that spoof an AP's transmission power can severely breach this limit. For example, an AP normally restricted to 10 dBm could be forced to transmit at the maximum of 36 dBm, causing the I/N to increase to 20 dB, 2^{26} times higher than the threshold.

We demonstrate this threat with a simulation shown in Figure 6. By placing a compromised AP in Manhattan (-73.9851, 40.7589) and setting it to maximum transmission power, our model shows that 17 nearby FS receivers become negatively affected. By using the OpenAFC propagation model, which considers terrain data and receiver gain, our results realistically model this impact.

Interference to Radio Observatories. These Stand Power Wi-Fi APs can not only interfere with incumbent devices, but can also interfere with radio observatories to affect astronomical observations. FCC enforces exclusion zones for certain radio observatories in [10]. That means the AP should not transmit any signal on 6650-6675.2 MHz in the calculated exclusion zones. However, with our GPS spoofing attack, we can bypass this limit and cause harm to the observatories. Figure 15 shows our simulation of the exclusion zone. If the AP is placed inside these zones, its transmitter will have a line-of-sight propagation path to the observatory antennas and create potential interference.

6.2.2 Wi-Fi Spoofing Efficiency

We evaluated the efficacy of our spoofing implementation by measuring the proportion of spoofed Wi-Fi networks successfully injected into the Ubiquiti AP's location requests. We conducted experiments under two conditions: transmitting the spoofing signal on the AP's current operating channel and on a different channel. After transmitting spoofing signals for one minute with a specific number of MAC addresses, we triggered a location request. As detailed in Table 2, the

# spoofed	50	100	200	500
% received current channel	100%	100%	92.75%	56.85%
% received other channel	88%	66.5%	36%	16%

Table 2: Percentage of Spoofed MAC in the Location Request

percentage of captured addresses decreases as the volume of spoofed APs increases. These results indicate that while our spoofing is highly effective on the AP's operating channel, attacks on other channels may fail to inject a sufficient number of MAC addresses to alter the AP's location. Additionally, we observed that the ASUS AP employs a distinct Wi-Fi geolocation implementation, aggregating multiple scans to identify and rely on a limited set of the most frequently observed MAC addresses. To succeed, we had to limit the volume of spoofed APs. This suggests that effective attacks against these devices

```
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 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 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
```

Listing 3: Max EIRP of AFC Channel

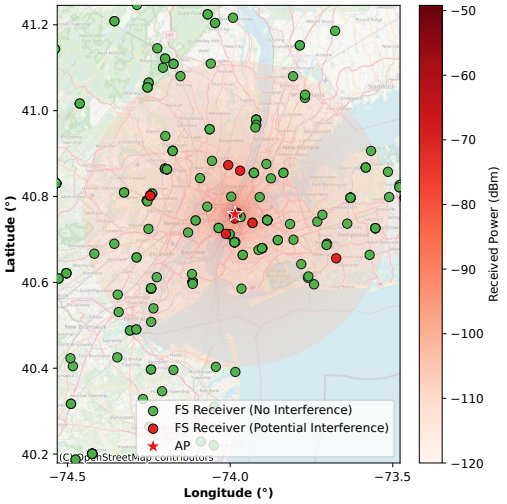

Figure 6: Interference Caused by AP

require a tailored strategy based on a specific analysis of their Wi-Fi geolocation implementations.

In addition, we evaluate the feasibility of Wi-Fi spoofing across the five largest metropolitan areas in the U.S. by determining the threshold of spoofed APs required to alter the target's calculated location. For these experiments, we constructed location requests containing 188 authentic Wi-Fi networks observed at the true location, augmented with varying numbers of spoofed networks associated with the target location. As shown in Figure 7, an attacker must simulate between 80 and 300 unique Wi-Fi networks to successfully shift the AP's location. The red-hatched regions in the figure represent an uncertainty interval in which the density of spoofed signals is sufficient to disrupt the true location fix but insufficient to establish a falsified one; in these cases, the location server is unable to determine any location. Furthermore, spoofing a target location in a rural area presents a greater challenge, as the scarcity of registered Wi-Fi networks in those regions limits the number of valid spoofed MAC addresses an attacker can generate, often making it impossible to overpower the authentic signals in a dense urban environment.

6.3 Denial-of-Service (DoS) Attacks

6.3.1 A2: DoS Attack Using a Foreign Location

We observed that when spoofing the AP to a foreign location outside of the United States, all the transmissions in the 6 GHz

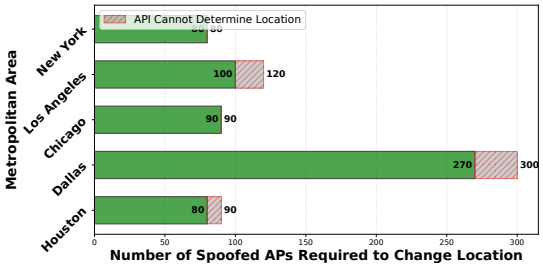

Figure 7: Number of APs Required to Spoof the Location

bands are disabled. We used the coordinate (30, 120) located in China. China does not permit the use of 6 GHz frequencies yet, and the AFC system is not available. As a result, the AFC server returns an empty list of allowed channels, causing the AP to stop transmission immediately.

```
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
```

Listing 4: Received AFC Channels of **A2**-**A5** from Aruba AP

6.3.2 A3: DoS Attack Using Invalid Location Timestamp

When we injected spoofed GPS signals whose embedded timestamps did not align with the AP's current time, the tested APs failed to receive any response from the AFC server. This behavior is independent of time zones because the server compares absolute timestamps rather than local times. Listing 4 shows an example console message from the Aruba AP indicating that no channels were provisioned. This timestamp check might be a deliberate defense against replayed or stale location reports. However, in practice, it is insufficient to defend against spoofed locations. Attacks **A2** and **A3** result in the AP receiving no valid 6 GHz allocation and must cease transmissions, resulting in a denial-of-service for affected clients, even when the AP is physically located in a non-protected area.

6.3.3 A4: DoS Attack Using Invalid Network Time

Similar to **A3**, the APs require an accurate time for the AFC operations. All 4 APs tested use the NTP protocol to sync their time to upstream time servers. Among them, only the RUCKUS AP is using Network Time Security (NTS), which provides authentication and encryption to NTP traffic. The other 3 APs are using plaintext NTP protocol, as shown in 12 in Appendix C. If they are not synced with a time server, we can spoof the traffic and control the time of the AP.

6.3.4 A5: DoS Attack Using DNS Poisoning

During our tests, we found all 4 APs issued plaintext DNS queries. Because these DNS lookups are unauthenticated, an off-path network attacker can forge or poison DNS responses so that the AP resolves AFC or other dependency (e.g., NTP) hostnames to invalid addresses (causing failures) or to attacker-controlled hosts (enabling further manipulation). Either outcome can prevent the AP from receiving a valid *availableSpectrumInquiryResponse* and thus block channel/power assignment. DNS hijacking also enables additional attacks, for example, redirecting the AP to an attacker-controlled NTP server that supplies malicious time values and triggers the forced re-query to AFC servers (**A6**). Figure 13 in Appendix C shows an example of plaintext DNS traffic captured from a Ubiquiti U7 Pro device.

6.3.5 Impact of DoS Attacks

Similar to the interference attack, traditional signal jammers must continuously broadcast high-power noise to deny spectrum access, rendering them readily detectable by spectrum monitoring systems [66]. In contrast, discussed attacks deny service by exploiting semantic vulnerabilities in the AFC coordination protocol rather than injecting sustained RF energy into the channel. These attacks remain structurally valid within the protocol and require only brief transmission windows to trigger prolonged denial effects. For example, a successful location spoofing attack may require only minutes of low-power transmission, yet it can induce harmful interference or service denial lasting more than 24 hours, for the duration of an AFC lease. This transient transmission significantly reduces the attacker's RF footprint. Unlike a jammer's persistent, high-energy emissions, our attacks rely on short-lived manipulation of control-plane inputs, making them substantially harder to detect, localize, and attribute using conventional spectrum monitoring techniques.

6.4 A6: Force Location Update Attack

Different from attack **A1**–**A5**, which exploits flaws in the AFC design and is generic to all the APs, **A6** presents an implementation-specific issue that compromises the security. We independently discovered an attack that exploits a known flaw in the AP's NTP client (NTP Bug 3596, CVE-2020-13817 [47]). By continuously responding to the AP's periodic NTP requests with spoofed NTP responses whose timestamps differ drastically from the AP's internal clock (we reproduced the effect by delivering eight consecutive spoofed responses over roughly ten minutes), the AP's `ntpdate` client crashes. The crash then causes the device to perform an immediate time resynchronization and to re-issue an *availableSpectrumInquiryRequest* to the AFC server. This forced re-query enables an off-path attacker to trigger the location- and time-manipulation attacks described in **A1**–**A5** at arbitrary times, rather than waiting for normal lease expiration or scheduled updates. With the ability to force immediate re-requests, an attacker can **(1)** induce incorrect time/location behavior (leading to denial-of-service or incorrect channel assignments) and **(2)** increase the frequency of AFC requests, potentially enabling load-based disruption, which we did not experimentally evaluate for ethical reasons because it would require targeting production infrastructure.

We identified this failure behavior empirically on the Aruba AP and subsequently confirmed the issue matches the public CVE report. The upstream fix was released in `ntpdate` 4.2.8p14 (2022). However, the tested AP still ships with `ntpdate` 4.2.8p9 (2016) and has not received a firmware update that incorporates the fix. While other minor vulnerabilities exist in the device's outdated firmware, they did not produce crash behavior and therefore were not directly exploitable for this forced-update vector.

7 Attacks on AFC Servers & Impact Analysis

While §6 analyzes attacks impacting AP devices, the correct and robust operation of AFC servers is equally critical to overall spectrum coordination. Moreover, the input-manipulation attacks discussed earlier do not terminate at the AP, and the spoofed or malformed values are ultimately consumed by the AFC server, which performs centralized frequency and power calculations. Therefore, weaknesses in server-side validation or processing can amplify the impact of compromised AP inputs and potentially affect multiple APs or incumbent protection guarantees.

At the same time, active adversarial testing against production AFC infrastructure poses a risk of real-world disruption. Malicious or malformed requests could influence allocation decisions for APs outside our control and impact incumbent systems. For ethical reasons, we therefore refrain from sending malformed inputs to commercial AFC deployments. Instead, we adopt a complementary evaluation strategy that combines limited testing of commercial AFC deployments with controlled experiments on a self-hosted implementation. We issue controlled and rate-limited *benign* queries to commercial AFC endpoints to observe normal request/response behavior and identify potential protocol or configuration lapses without affecting service availability. In parallel, for repre-

sentative security testing, we deploy a self-hosted instance of the open-source OpenAFC implementation [48], part of the Telecom Infra Project (TIP). This allows us to inspect request/response flows, exercise edge cases, and conduct non-destructive experiments that would be inappropriate against production infrastructure. We deploy OpenAFC on a server equipped with two Intel Xeon Gold 6448H CPUs (64 Cores at 4.1 GHz) and 1 TB of memory.

7.1 Security Verification of AFC Servers

We verified the security measures of all 5 tested AFC servers (4 commercial and 1 open-source) and confirmed that they all complied with the security requirements in §3.2.

- **(AFC-M1)** All communications between the AP and the AFC server are protected by TLS (comply with **REQ1**).
- **(AFC-M2)** There is no interface for an entity outside of the AFC server (e.g., AP) to access or modify the AFC databases (comply with **REQ2**).
- **(AFC-M3)** For benign AP requests, a correct list of frequency and power allocation is computed and returned. (comply with **REQ3**).

7.2 Resource Exhaustion Attack on Servers

Although malformed or malicious inputs can trigger implementation-specific failures, including crashes and parsing bugs, these issues depend on particular server implementations and therefore fall outside the scope of our ethical testing of commercial infrastructure. Instead, we show that AFC response computation requires non-trivial work (incumbent lookups, spatial intersection checks, and constraint synthesis) and consumes considerable CPU and memory, and is thereby susceptible to resource exhaustion attacks.

7.2.1 Identifying the Most Impactful Attack Location

To representatively quantify and evaluate the resource-exhaustion costs, we first conduct a controlled experiment on OpenAFC [48]. To assess the impact of queries on AFC server resources, we tested locations within the 10 largest U.S. metropolitan areas. The evaluation points were uniformly distributed, with a 5 km separation between each point. An example query payload can be found in Listing 7.

As the results shown in Table 3, the end-to-end API response time varies from 4 seconds to 18 seconds, with an average time of 8 seconds in the 10 largest metropolitan areas evaluated. Figure 14 provides a visualization of the coordinates evaluated, and Figure 8 provides the API response time in the Los Angeles metropolitan area.

We also find that the API response time is correlated with the number of incumbent devices nearby. By default, OpenAFC considers the incumbent devices within 150 kilometers. Figure 9 supports our results. Note that the API response times

Metropolitan	# Coord	Mean	Median	Min	Max	SD
New York	895	7.4867	8.1253	4.0900	14.1633	1.9494
Los Angeles	591	12.1689	12.1494	4.1010	18.1697	2.6838
Chicago	923	5.9535	6.1202	4.0918	8.1461	1.0049
Dallas	937	9.5790	10.1348	6.1139	14.1676	1.3526
Houston	1039	7.6426	8.1270	4.0975	12.1617	1.5270
Miami	619	5.7192	6.1190	4.0886	10.1428	1.4446
Washington	655	9.9001	10.1401	8.1112	14.1645	1.4383
Atlanta	925	5.0983	4.1252	4.0863	8.1401	1.0272
Philadelphia	499	9.9265	10.1361	6.1058	16.3582	1.9229
Phoenix	1476	7.5151	8.1256	4.1071	10.7057	1.2802
Overall	8559	7.8385	8.1263	4.0863	18.1697	2.4834

Table 3: API Response Time (in Seconds) on the 10 Largest Metropolitan Areas in the U.S.

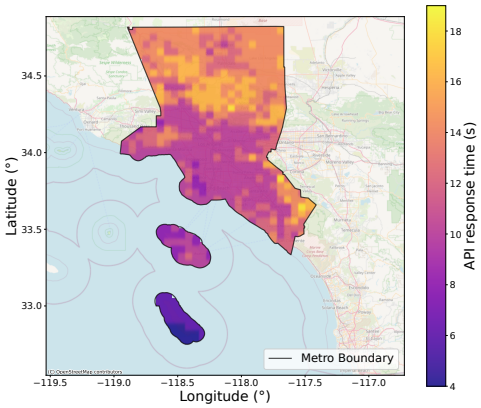

Figure 8: LA API Response Time Heatmap

are always a multiple of 2 seconds in our results, since the implementation pulls the computed results with a 2-second interval and then provides the response. An attacker can likewise query the more resource-demanding locations and use the inferred locations to launch a resource starvation attack on the AFC server.

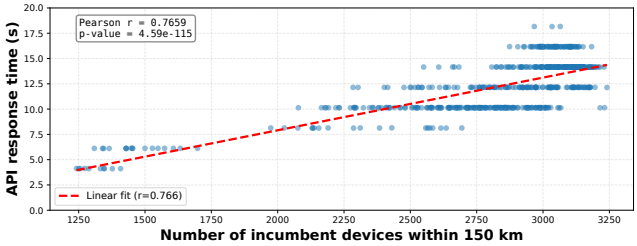

Figure 9: Correlation between API Response Time and Number of In-Range Incumbent Devices

7.2.2 Impact of Concurrent Requests

Attack **A6** discussed in §6.4 shows that an attacker can force the AP to update its AFC channel at arbitrary times. To study the server-side impact of this capability, we simulated an attack that issues large numbers of concurrent *availableSpectrumInquiryRequest* messages targeted at locations that maximize server work (regions with dense incumbent lists). OpenAFC enqueues incoming requests and performs the full geometry/policy computation before producing an *availableSpectrumInquiryResponse*. Figure 10 plots end-to-end API

response time as a function of concurrent requests. When the server becomes saturated, many requests exceed OpenAFC's default 180 s processing window and are discarded with HTTP 504 (Gateway Timeout). In our experiments, once concurrency reached the order of 1,000 simultaneous requests, a large fraction of requests were timed out and effectively dropped, preventing benign APs that coincide with that interval from receiving timely channel allocations.

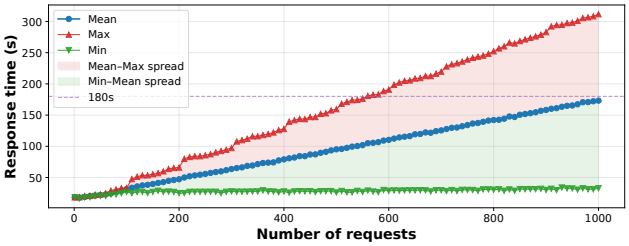

Figure 10: API Response Time vs # of Concurrent Requests

When the server is busy serving a burst of attacker-triggered re-requests, APs that are not under direct attack can still be denied service because their legitimate queries are delayed or dropped. If an operator relies on a small number of centralized AFC instances, such an attack could affect many APs across a wide geographic area (or many customers served by a provider), producing region-scale service disruption.

7.2.3 Validation on Commercial AFC Server

To validate our findings on production infrastructure, we conducted a limited-scale experiment (due to ethical concerns) targeting the commercial AFC servers operated by Qualcomm [50] and the Wi-Fi Alliance (WFA) [61]. We randomly sampled geographic coordinates within the United States and measured the end-to-end API response time for *availableSpectrumInquiryRequest* queries. To ensure ethical testing and prevent potential service degradation, we strictly rate-limited our requests to avoid resource exhaustion.

The results, presented in Figure 11, demonstrate a positive correlation between API response time and the number of nearby incumbent devices for both commercial AFC implementations. The WFA AFC, which utilizes the OpenAFC codebase, exhibits performance characteristics and latency trends comparable to our self-hosted instance discussed in §7.2.1. In contrast, Qualcomm's implementation displays a weaker correlation and faster overall response times, suggesting the use of more substantial hardware resources or aggressive caching mechanisms.

Despite the performance differences, the observable dependency between incumbent density and API response time confirms that commercial implementations remain susceptible to the resource exhaustion vectors. While ethical constraints prevented us from executing a high-volume flooding attack, the data suggests that a sustained influx of complex queries would impose significant processing overhead, potentially

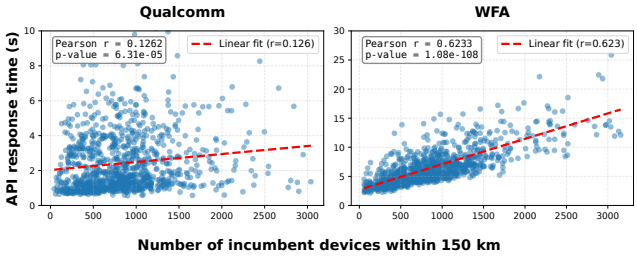

Figure 11: API Response Time of Commercial AFC Servers

resulting in a denial-of-service condition for legitimate users.

8 Potential Threat Mitigations

Developing effective defenses against the attacks on AFC systems is non-trivial because deployment costs directly conflict with stakeholders' cost-efficiency goals. In this section, we discuss practical mitigations that enhance AFC security without necessitating a fundamental redesign of the specifications or compromising user experience. Since the system's primary objective is to prevent interference with incumbent services, we recommend that vendors prioritize the detection of location spoofing and disable 6 GHz operations when anomalies are detected. Table 4 summarizes these proposed mitigations.

Mitigations	Firmware	Hardware	Cloud	Positioning System
Geofencing	✗	✗	✓	✗
Multiple Location Sources	✓	✗	✗	✗
Physical-Level Spoofing Detection	✓	✓	✗	✗
Coordinated Detection	✓	✗	✓	✗
Authenticate Localization Messages	✗	✗	✗	✓
Use secure DNS and NTP protocols	✓	✗	✗	✗
Update dependency	✓	✗	✗	✗

Table 4: Summary of Proposed Mitigations
✓: Require change ✗: Does not require change

8.1 Mitigation of Location Spoofing Attacks

Location spoofing attacks in the AFC system stem from the use of unauthenticated GPS and Wi-Fi signals. Since upgrading global satellite infrastructure or altering Wi-Fi protocols to support authentication is not feasible in the short term, we propose layered mitigations. These measures aim to substantially raise the attacker's cost and complexity while improving the detectability of spoofing attempts.

Geofencing. Given that fundamental updates to positioning systems are infeasible in the short term, geofencing offers a cost-effective defense against location spoofing. In typical Wi-Fi deployments, most APs remain at fixed coordinates with negligible variation. Leveraging this stationarity, AFC providers can establish a geofence [53] around an AP's reported location during its initial setup. If the AP subsequently reports a location outside this expected boundary, the system can flag the anomaly and suspend 6 GHz service. This solution is practical to deploy, requiring only a feature update

to the vendor's cloud management interface and a one-time configuration step during device provisioning. In our conversation with the vendors, HPE Aruba mentioned they are discussing implementing the geofencing feature as a part of their cloud controller.

Multiple Location Sources. To enhance resilience against location spoofing, APs should not rely on a single location source. Instead, fusing GNSS and Wi-Fi positioning significantly raises the bar for attackers, as they would need to spoof both signals simultaneously to succeed. Since standard APs are already equipped with Wi-Fi radios and GNSS receivers, implementing this dual-source verification is primarily a software update rather than a hardware overhaul. Existing frameworks like Android's Fused Location API [29] and recent research such as Guardian [43] demonstrate the effectiveness of using multiple sources to detect anomalies. However, this approach introduces a trade-off: strict cross-verification means that if either signal is unavailable or inconsistent, the AP may be forced to disable 6 GHz operation, potentially leading to increased service disruptions for legitimate users.

Physical-Level Spoofing Detection. Detecting spoofing signals in-device is another possible solution. Since all GPS signals come from satellites, a GPS receiver may calculate the signal Angle-of-Arrival (AoA) for spoof detection. From the AoA, the receiver can discriminate between signals coming from above and signals coming from an attacker on the ground. A recent work [42] implements this defense mechanism in COTS GPS chips. In the context of Wi-Fi, similar works [65] have utilized AoA and physical-layer channel state information (CSI) to detect spoofing by verifying that the signal originates from the AP's claimed spatial direction. However, standard GPS and Wi-Fi positioning implementations do not currently support this feature. Implementing these methods typically requires hardware changes (e.g., antenna arrays) or low-level firmware access, which may increase the cost and complexity of the devices.

Coordinated Detection. Multi-receiver arrays effectively detect single-antenna GPS spoofers by identifying relative position distortions [41]. Since Wi-Fi APs are typically deployed in clusters, they can function as a distributed array, allowing the AFC system to flag anomalies where GPS-derived inter-AP distances contradict the deployment topology. This coordinated approach also mitigates Wi-Fi spoofing by enforcing spatial consistency through aggregated neighbor lists and RSSI data; for instance, the system can detect an AP reporting neighbors that are invisible to adjacent peers [31]. Crucially, this is a software-only solution implemented at the cloud controller, requiring no hardware modifications.

Authenticate Localization Messages. The lack of authentication in localization messages is the fundamental vulnerability enabling location spoofing. Implementing authentication schemes within these systems would allow APs to verify the origin of location data, thereby neutralizing the attacks described in this work. This approach is consistent with the AFC trust assumptions outlined in §3.1 and preserves system usability. While authentication mechanisms for GPS have been proposed [67], civilian signals remain unauthenticated, and full deployment likely hinges on comprehensive satellite constellation updates. Similarly, authentication protocols have been suggested for cellular networks [21]. In the long term, the adoption of these trusted positioning systems is crucial for securing the diverse ecosystem of dependent operations.

8.2 Mitigation of Other Attacks

Use Secure DNS and NTP Protocols. Network-based attacks like NTP and DNS spoofing can be prevented by enforcing encrypted traffic. Network Time Security (NTS) [26] provides authenticated time synchronization. For DNS, DNSSEC [33] ensures authenticity, while DNS over TLS (DoT) [37] and DNS over HTTPS (DoS) [34] encrypt queries. Despite these standards, adoption remains low, with over 88% of global queries still sent in plaintext [18]. To secure Wi-Fi APs, vendors must prioritize encrypting all communications between the AP and backend servers.

Update Dependency. The security of legacy subsystems is frequently overlooked. For instance, we identify an outdated NTP client with n-day vulnerabilities in the HPE Aruba AP (§6.4). Vendors must ensure the timely adoption of security fixes across all software layers.

9 Conclusion

The 6 GHz band enables high-performance Wi-Fi connectivity, but its safe and compliant operation depends on the integrity of the AFC systems. While AP-AFC communications are secured, our systematic security analysis shows that AFC's reliance on unauthenticated inputs, including location, DNS, and time, creates practical off-path vectors, allowing attackers to manipulate AP-reported location, bypass spectrum restrictions, and disrupt incumbent services. We validated these attacks on commercial APs and studied the implications for AFC servers, demonstrating that current protections are not sufficient to defend against input-level manipulation. These findings expose critical vulnerabilities in AFC's trust model and highlight the broader risks of insecure sensor inputs. To ensure the reliability of spectrum sharing, future designs should incorporate mechanisms for robust and verifiable location reporting along with network-level defenses.

Acknowledgments

We thank our shepherd, Dr. Amin Vahdat, and the anonymous reviewers for their valuable feedback and guidance. We are grateful to David Waters, Tim Godfrey, and Jay Herman at the Electric Power Research Institute (EPRI); Dr. Muhammad Rochman and Dr. Monisha Ghosh from the University of Notre Dame; Dr. Thomas Willis from AT&T Labs; David Hattey from Lockard & White; and John Beck from Idaho National Laboratory for their technical assistance with the test AP setup and helpful discussions. This work is supported by a research grant from the Department of Energy (DOE) Office of the Cybersecurity, Energy Security, and Emergency Response (CESER), in collaboration with Idaho National Laboratory (INL).

Ethical Considerations

All experiments were performed in confined, controlled environments where only equipment under our control was affected. Active RF tests and any GNSS/GPS spoofing were conducted in isolated testbeds where over-the-air transmissions were limited in power, duration, and frequency to avoid affecting third parties. We did not perform malicious experiments on operational public networks. Vulnerabilities discovered in commercial APs were reported to vendors (e.g., HPE, RUCKUS, Ubiquiti). Exploit-level artifacts will be withheld until vendors confirm mitigations or an agreed disclosure timeline. We tested only open-source AFC servers that we deployed ourselves and did not submit malicious inputs to commercial AFC servers or otherwise take actions that could disrupt production services.

Availability

This work focuses on systematic threat analysis on AFC systems (both the AP and server), and we will open-source all test-related artifacts to facilitate future research. Subject to responsible disclosure and safety considerations, we will release sanitized experiment harnesses and automation scripts (including OpenAFC server test scripts), configurations, benign sample payloads, sanitized input/output traces and telemetry, and documentation describing how to reproduce and interpret the experiments.

References

[1] Access Point U7 Pro Outdoor. https://store.ui.com/us/en/products/u7-pro-outdoor-us.

[2] HPE Aruba Networking AP-634 (US) Tri-radio 2x2:2 Wi-Fi 6E External Antennas Campus AP. https://buy.hpe.com/us/en/networking/wireless-devices/wlan-access-points/hpe-aruba-networking-ap%E2%80%91634-us-tri%E2%80%91radio-2x2:2-wi%E2%80%91fi-6e-external-antennas-campus-ap/p/s1g50a.

[3] Rog strix gs-be18000 | networking | rog global. https://rog.asus.com/networking/rog-strix-gs-be18000/. Accessed: 2026-01-23.

[4] RUCKUS T670 Outdoor Access Point. https://www.ruckusnetworks.com/products/wireless-access-points/t670/.

[5] USRP B210. https://www.ettus.com/all-products/ub210-kit/.

[6] Usrp b2x0 series hardware driver and usrp manual. https://files.ettus.com/manual/page_usrp_b200.html#b200_hw_ref_ext. Accessed: 2026-02-16.

[7] 47 C.F.R. part 96 - Citizens Broadband Radio Service. https://www.ecfr.gov/current/title-47/part-96, 2015.

[8] 47 C.F.R. § 96.39(c)(2) – Citizens Broadband Radio Service Device (CBSD) general requirements. https://www.ecfr.gov/current/title-47/section-96.39, 2015.

[9] 47 C.F.R. § 101.3 - Definitions. https://www.ecfr.gov/current/title-47/chapter-I/subchapter-D/part-101/subpart-A/section-101.3, 2020.

[10] 47 C.F.R. § 15.407 - general technical requirements. https://www.ecfr.gov/current/title-47/chapter-I/subchapter-A/part-15/subpart-E/section-15.407, 2024.

[11] Mayank Agarwal, Santosh Biswas, and Sukumar Nandi. Discrete event system framework for fault diagnosis with measurement inconsistency: Case study of rogue dhcp attack. *IEEE/CAA Journal of Automatica Sinica*, 6(3):789–806, 2017.

[12] Dennis M Akos and James BY Tsui. Design and implementation of a direct digitization gps receiver front end. *IEEE Transactions on Microwave Theory and Techniques*, 44(12):2334–2339, 1996.

[13] Manar Aldaoud, Dawood Al-Abri, Ahmed Al Maashri, and Firdous Kausar. Dhcp attacking tools: an analysis. *Journal of Computer Virology and Hacking Techniques*, 17(2):119–129, 2021.

[14] Arupjyoti Bhuyan, Mingyue Xi, Xiang Zhang, Sneha Kasera, and Shamik Sarkar. Secure mmwave spectrum sharing with autonomous beam scheduling for 5g and beyond. Technical report, Idaho National Laboratory (INL), Idaho Falls, ID (United States), 2022.

[15] Bastian Bloessl, Michele Segata, Christoph Sommer, and Falko Dressler. An ieee 802.11 a/g/p ofdm receiver for gnu radio. In *Proceedings of the second workshop on Software radio implementation forum*, pages 9–16, 2013.

[16] Bobzilla, Arkasha, and Uhtu. WiGLE: Wireless Network Mapping. https://wigle.net/, 2026. Accessed: 2026-01-13.

[17] Xiang Cheng, Hanchao Yang, Shinan Liu, and Yaling Yang. Distributed multi-antenna gps spoofing attack using off-the-shelf devices. In *18th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pages 28–39, 2025.

[18] Cloudflare. DNS queries to 1.1.1.1. https://radar.cloudflare.com/dns?dateRange=24w, 2025. Accessed: 2025-09-10. Data for the preceding 24 weeks.

[19] José A del Peral-Rosado, Ronald Raulefs, José A López-Salcedo, and Gonzalo Seco-Granados. Survey of cellular mobile radio localization methods: From 1g to 5g. *IEEE Communications Surveys & Tutorials*, 20(2):1124–1148, 2017.

[20] Seda Dogan-Tusha, Armed Tusha, Muhammad Iqbal Rochman, Hossein Nasiri, Joshua Roy Palathinkal, Mike Atkins, and Monisha Ghosh. Evaluation of indoor/outdoor sharing in the unlicensed 6 ghz band. In *2025 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, pages 1–9. IEEE, 2025.

[21] Yilu Dong, Rouzbeh Behnia, Attila A Yavuz, and Syed Rafiul Hussain. Securing 5G bootstrapping: A two-layer IBS authentication protocol. *arXiv preprint arXiv:2502.04915*, 2025.

[22] Yilu Dong, Tianchang Yang, Arupjyoti Bhuyan, and Syed Rafiul Hussain. GPS spoofing attacks on automated frequency coordination system in Wi-Fi 6E and beyond. *arXiv preprint arXiv:2509.02824*, 2025.

[23] Wenlong Du, Jian Li, Yanhao Wang, Libo Chen, Ruijie Zhao, Junmin Zhu, Zhengguang Han, Yijun Wang, and Zhi Xue. Vulnerability-oriented testing for {RESTful}{APIs}. In *33rd USENIX Security Symposium (USENIX Security 24)*, pages 739–755, 2024.

[24] Takuji Ebinuma. osqzss/gps-sdr-sim: Software-defined gps signal simulator. https://github.com/osqzss/gps-sdr-sim.

[25] Federal Communications Commission. Unlicensed Use of the 6 GHz Band Report and Order and Further Notice of Proposed Rulemaking ET Docket No. 18-295; GN Docket No. 17-183. Technical Report FCC 20-51, Federal Communications Commission, apr 2020. 35 FCC Rcd 3852.

[26] Daniel Fox Franke, Dieter Sibold, Kristof Teichel, Marcus Dansarie, and Ragnar Sundblad. Network Time Security for the Network Time Protocol. RFC 8915, September 2020.

[27] Phillipa Gill, Yashar Ganjali, and Bernard Wong. Dude, where's that {IP}? circumventing measurement-based {IP} geolocation. In *19th USENIX Security Symposium (USENIX Security 10)*, 2010.

[28] Sharon Goldberg, Miro Haller, Nadia Heninger, Mike Milano, Dan Shumow, Marc Stevens, and Adam Suhl. {RADIUS/UDP} considered harmful. In *33rd USENIX Security Symposium (USENIX Security 24)*, pages 7429–7446, 2024.

[29] Google. Fused location provider api. https://developers.google.com/location-context/fused-location-provider.

[30] Great Scott Gadgets. Hackrf pro. https://greatscottgadgets.com/hackrf/pro/.

[31] Xiao Han, Junjie Xiong, Wenbo Shen, Zhuo Lu, and Yao Liu. Location heartbleeding: The rise of wi-fi spoofing attack via geolocation api. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, pages 1383–1397, 2022.

[32] Haibo He and Jun Yan. Cyber-physical attacks and defences in the smart grid: a survey. *IET Cyber-Physical Systems: Theory & Applications*, 1(1):13–27, 2016.

[33] Paul E. Hoffman. DNS Security Extensions (DNSSEC). RFC 9364, February 2023.

[34] Paul E. Hoffman and Patrick McManus. DNS Queries over HTTPS (DoH). RFC 8484, October 2018.

[35] Rebekah Houser, Shuai Hao, Zhou Li, Daiping Liu, Chase Cotton, and Haining Wang. A comprehensive measurement-based investigation of dns hijacking. In *2021 40th International Symposium on Reliable Distributed Systems (SRDS)*, pages 210–221. IEEE, 2021.

[36] Jiangqi Hu, Sabarish Krishna Moorthy, Ankush Harindranath, Zhaoxi Zhang, Zhiyuan Zhao, Nicholas Mastronarde, Elizabeth Serena Bentley, Scott Pudlewski, and Zhangyu Guan. A mobility-resilient spectrum sharing framework for operating wireless uavs in the 6 ghz band. *IEEE/ACM Transactions on Networking*, 31(6):3128–3142, 2023.

[37] Zi Hu, Liang Zhu, John Heidemann, Allison Mankin, Duane Wessels, and Paul E. Hoffman. Specification for DNS over Transport Layer Security (TLS). RFC 7858, May 2016.

[38] Syed Rafiul Hussain, Omar Chowdhury, Shagufta Mehnaz, and Elisa Bertino. LTEInspector: A systematic approach for adversarial testing of 4g LTE. In *25th Annual Network and Distributed System Security Symposium, NDSS, 2018*. The Internet Society.

[39] Institute of Electrical and Electronics Engineers. IEEE Standard for Information Technology–Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks–Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Enhancements for High-Efficiency WLAN. Technical Report IEEE Std 802.11ax-2021, IEEE, feb 2021.

[40] Institute of Electrical and Electronics Engineers. IEEE Approved Draft Standard for Information technology–Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment: Enhancements for Extremely High Throughput (EHT). Technical Report IEEE Std 802.11be-2024, IEEE, sep 2024.

[41] Kai Jansen, Nils Ole Tippenhauer, and Christina Pöpper. Multi-receiver gps spoofing detection: Error models and realization. In *Proceedings of the 32nd Annual Conference on Computer Security Applications*, pages 237–250, 2016.

[42] Shinan Liu, Xiang Cheng, Hanchao Yang, Yuanchao Shu, Xiaoran Weng, Ping Guo, Kexiong Curtis Zeng, Gang Wang, and Yaling Yang. Stars can tell: a robust method to defend against {GPS} spoofing attacks using off-the-shelf chipset. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 3935–3952, 2021.

[43] Wenjie Liu and Panos Papadimitratos. Guardian positioning system (gps) for location based services. In *18th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pages 88–99, 2025.

[44] Aanchal Malhotra, Isaac E Cohen, Erik Brakke, and Sharon Goldberg. Attacking the network time protocol. *Cryptology ePrint Archive*, 2015.

[45] James A Muir and Paul C Van Oorschot. Internet geolocation: Evasion and counterevasion. *Acm computing surveys (csur)*, 42(1):1–23, 2009.

[46] National Institute of Standards and Technology. ESC Sensor Detection and Placement. https://www.nist.gov/ctl/wirelessnet/esc-sensor-detection-and-placement, July 2022. Accessed: 2026-01-23.

[47] Network Time Foundation. Ntp bug 3596: Unauthenticated and unmonitored ntpd may be susceptible to ipv4 attack from highly predictable transmit timestamps, March 2020. https://www.ntp.org/support/securitynotice/ntpbug3596/.

[48] Open AFC Project. open-afc-project/openafc. https://github.com/open-afc-project/openafc.

[49] Yarin Perry, Neta Rozen Schiff, and Michael Schapira. A devil of a time: How vulnerable is ntp to malicious timeservers? In *NDSS*, 2021.

[50] Qualcomm Technologies, Inc. Taking Wi-Fi to new heights: FCC's advancement of standard power and automated frequency coordination. https://www.qualcomm.com/news/onq/2024/02/taking-wi-fi-to-new-heights-fcc-advances-standard-power-and-automated-frequency-coordination, 2024. Accessed: 2026-02-17.

[51] Qualcomm Technologies, Inc. Unlocking 6ghz wi-fi's full potential: Qualcomm dragonwing automated frequency coordination (afc) suite. April 2025.

[52] Recon Analytics. Cbrs: An unproven spectrum sharing framework. Technical report, CTIA, November 2022.

[53] Sandro Rodriguez Garzon and Bersant Deva. Geofencing 2.0: taking location-based notifications to the next level. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, pages 921–932, 2014.

[54] Altaf Shaik, Ravishankar Borgaonkar, N Asokan, Valtteri Niemi, and Jean-Pierre Seifert. Practical attacks against privacy and availability in 4g/lte mobile communication systems. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, 2016.

[55] Shanghao Shi, Yang Xiao, Wenjing Lou, Chonggang Wang, Xu Li, Y Thomas Hou, and Jeffrey H Reed. Challenges and new directions in securing spectrum access systems. *IEEE Internet of Things Journal*, 8(8):6498–6518, 2021.

[56] Christopher Tibaldo, Harshad Sathaye, Giovanni Camurati, and Srdjan Capkun. Gnss-wasp: Gnss wide area spoofing. In *USENIX Security 2025*, 2025.

[57] Nils Ole Tippenhauer, Christina Pöpper, Kasper Bonne Rasmussen, and Srdjan Capkun. On the requirements for successful gps spoofing attacks. In *Proceedings of the 18th ACM conference on Computer and communications security*, pages 75–86, 2011.

[58] Nils Ole Tippenhauer, Kasper Bonne Rasmussen, Christina Pöpper, and Srdjan Čapkun. Attacks on public

wlan-based positioning systems. In *Proceedings of the 7th international conference on Mobile systems, applications, and services*, pages 29–40, 2009.

[59] Kang Wang, Shuhua Chen, and Aimin Pan. Time and position spoofing with open source projects. *black hat Europe*, 148:1–8, 2015.

[60] Wi-Fi Alliance. Afc system to afc device interface specification. Technical Report 1.5, Wi-Fi Alliance, May 2023.

[61] Wi-Fi Alliance. Wi-Fi AFC: Supercharge 6 GHz Wi-Fi. https://www.wi-fi.com/wi-fi-afc, 2024. Accessed: 2026-02-17.

[62] Wireless Innovation Forum. Requirements for CBRS Certified Professional Installer (CPI). Technical Report WINNF-TS-0247, Wireless Innovation Forum, apr 2024.

[63] Wireless Innovation Forum. Functional requirements for the U.S. 6 ghz band under the control of an afc system. Technical Report WINNF-TS-1014, Wireless Innovation Forum, apr 2025.

[64] Yuhao Wu, Jinwen Wang, Yujie Wang, Shixuan Zhai, Zihan Li, Yi He, Kun Sun, Qi Li, and Ning Zhang. Your firmware has arrived: A study of firmware update vulnerabilities. In *33rd USENIX Security Symposium (USENIX Security 24)*, pages 5627–5644, 2024.

[65] Jie Xiong and Kyle Jamieson. Securearray: Improving wifi security with fine-grained physical-layer information. In *Proceedings of the 19th annual international conference on Mobile computing & networking*, pages 441–452, 2013.

[66] Wenyuan Xu, Wade Trappe, Yanyong Zhang, and Timothy Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*, pages 46–57, 2005.

[67] Muzi Yuan, Xiaomei Tang, and Gang Ou. Authenticating gnss civilian signals: A survey. *Satellite Navigation*, 4(1):6, 2023.

A Example API Request and Response Messages

```
{
  "version": "1.4",
  "availableSpectrumInquiryRequests": [
    {
      "requestId": "1964925685",
      "deviceDescriptor": {
        "serialNumber": "1616555555",
        "certificationId": [
          {
            "rulesetId": "US_47_CFR_PART_15_SUBPART_E",
            "id": "SWX-U7PRO0"
          }
        ]
      },
      "location": {
        "ellipse": {
          "center": {
            "longitude": -77.868436000000003,
            "latitude": 40.793517000000001
          },
          "majorAxis": 41,
          "minorAxis": 41,
          "orientation": 0
        },
        "elevation": {
          "height": 4.0,
          "heightType": "AMSL",
          "verticalUncertainty": 4
        },
        "indoorDeployment": 2
      },
      "inquiredFrequencyRange": [
        {
          "lowFrequency": 5945,
          "highFrequency": 6425
        },
        {
          "lowFrequency": 6525,
          "highFrequency": 6865
        }
      ],
      "inquiredChannels": [
        {
          "globalOperatingClass": 131,
          "channelCfi": [
            1,
            5,
            ...
          ]
        },
        ...
      ],
      "minDesiredPower": -10
    }
  ]
}
```

Listing 5: Example *availableSpectrumInquiryRequest*

```
{
  "version": "1.4",
  "availableSpectrumInquiryResponses": [
    {
      "requestId": "1964925685",
      "response": {
        "responseCode": 0,
        "shortDescription": "Success"
      },
      "rulesetId": "US_47_CFR_PART_15_SUBPART_E",
      "availableFrequencyInfo": [
        {
          "frequencyRange": {
            "lowFrequency": 5945,
            "highFrequency": 5991
          },
          "maxPsd": 19.4
        },
        ...
      ],
      "availableChannelInfo": [
        {
          "globalOperatingClass": 131,
          "channelCfi": [
            1,
            5,
            ...
          ],
          "maxEirp": [
            32.4,
            32.4,
            ...
          ]
        },
        ...
      ],
      "availabilityExpireTime": "2025-09-18T18:58:56Z"
    }
  ]
}
```

Listing 6: Example *availableSpectrumInquiryResponse*

```
{
    "version": "1.4",
        "availableSpectrumInquiryRequests": [{
            "requestId": request_id,
            "location": {
                "ellipse": {
                    "center": {
                        "latitude": latitude,
                        "longitude": longitude
                    },
                    "majorAxis": 100,
                    "minorAxis": 50,
                    "orientation": 45
                },
                "elevation": {
                    "height": 3,
                    "heightType": "AGL",
```

```
                "verticalUncertainty": 2
            },
            "indoorDeployment": 0
        },
        ...
    }]
}
```

Listing 7: Query Payload for Server Experiments (Unrelated Parameters Omitted)

B Addition Results on APs Tested

```
rkscli: get gps
GPS chip: AG3335M
GPS state: Enabled
GPS coordinates : 40.734388,-77.624202
Geo location source: gps
GPS last update at: 2026-01-02-01:29
GPS next update at: 2026-01-02-02:29
OK
```

Listing 8: Example GPS Information on RUCKUS AP

```
rkscli: get afc
AFC status: AFC passed with response
Power mode: SP
geo location:
  source type: GPS,  longitude: -77.624199,  latitude:
       40.734386,  major_axis: 25.00m,  minor_axis:
       25.00m
  height type: AGL  height: 8.75m  vertical_uncertainty:
       12.25m
OK
```

Listing 9: Example AFC Information on RUCKUS AP

```
{
    "skyhook": {
      "considerIp": "false",
      "hpeConfidence": 95,
      "includeLocationSource": "true",
      "wifiAccessPoints": [
        {
          "macAddress": "70:90:41:cc:68:e5",
          "frequency": 2412,
          "age": 29730,
          "signalStrength": -71
        },
        {
          "macAddress": "70:90:41:cc:66:a2",
          "frequency": 2412,
          "age": 29720,
          "signalStrength": -65
        },
        ...
    ]
}
```

Listing 10: Example Wi-Fi Location Request on Ubiquiti AP

```
{
    "location": {
        "lat": 40.714396,
        "lng": -74.006046
    },
    "accuracy": 162.8,
    "source": "wifi"
}
```

Listing 11: Example Wi-Fi Location Response on Ubiquiti AP

C Supplementary Figures

```
142.988601209 192.168.137.101 208.69.120.241   NTP      90 NTP Version 4, client
142.988663696 192.168.137.101 45.83.234.123    NTP      90 NTP Version 4, client
143.030169572 208.69.120.241  192.168.137.101 NTP      90 NTP Version 4, server
143.084969144 45.83.234.123   192.168.137.101 NTP      90 NTP Version 4, server
144.086442445 192.168.137.101 170.187.142.180 NTP      90 NTP Version 4, client
144.086478637 192.168.137.101 144.202.41.38   NTP      90 NTP Version 4, client
144.112959518 170.187.142.180 192.168.137.101 NTP      90 NTP Version 4, server
144.183869208 144.202.41.38   192.168.137.101 NTP      90 NTP Version 4, server
```

Figure 12: Plaintext NTP Traffic

```
DNS      79 Standard query 0x149f A 0.ubnt.pool.ntp.org
DNS      79 Standard query 0x149f A 0.ubnt.pool.ntp.org
DNS      79 Standard query 0x1b75 AAAA 0.ubnt.pool.ntp.org
DNS      79 Standard query 0x1b75 AAAA 0.ubnt.pool.ntp.org
DNS     191 Standard query response 0x9c49 AAAA 2.ubnt.pool.ntp.org AAAA 2604:2
DNS     134 Standard query response 0x1b75 AAAA 0.ubnt.pool.ntp.org SOA b.ntpns
DNS     143 Standard query response 0x149f A 0.ubnt.pool.ntp.org A 66.205.249.2
DNS     134 Standard query response 0x1b75 AAAA 0.ubnt.pool.ntp.org SOA e.ntpns
DNS     143 Standard query response 0x149f A 0.ubnt.pool.ntp.org A 173.71.69.15
DNS     143 Standard query response 0x58a5 A 1.ubnt.pool.ntp.org A 198.137.202.
DNS      83 Standard query 0x1586 A afcapi.qcs.qualcomm.com
DNS      83 Standard query 0x1586 A afcapi.qcs.qualcomm.com
DNS      83 Standard query 0x196e AAAA afcapi.qcs.qualcomm.com
DNS      83 Standard query 0x196e AAAA afcapi.qcs.qualcomm.com
DNS     131 Standard query response 0x1586 A afcapi.qcs.qualcomm.com A 52.40.20
DNS     161 Standard query response 0x196e AAAA afcapi.qcs.qualcomm.com SOA ns-
DNS     131 Standard query response 0x1586 A afcapi.qcs.qualcomm.com A 52.40.20
DNS     161 Standard query response 0x196e AAAA afcapi.qcs.qualcomm.com SOA ns-
```

Figure 13: Plaintext DNS Traffic

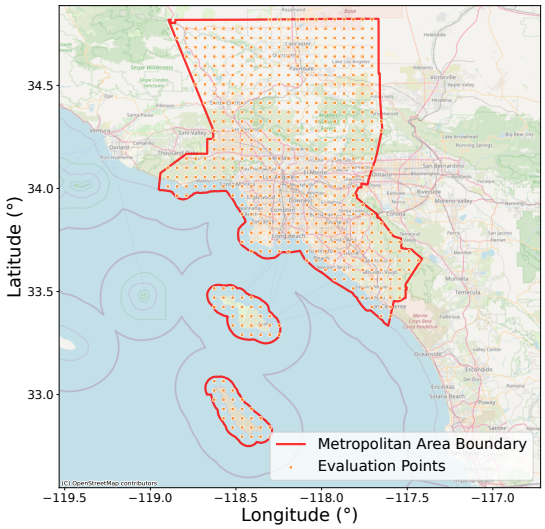

Figure 14: LA Evaluation Coordinates

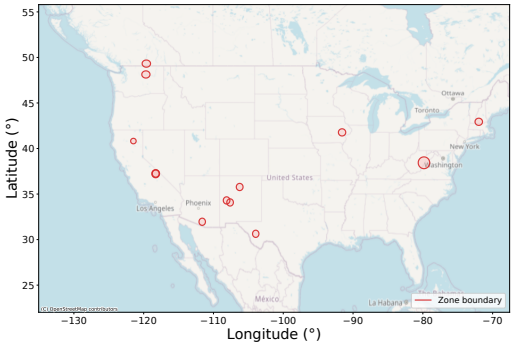

Figure 15: Exclusion Zone Computed by OpenAFC