Practical Attacks on AFC Clients in Wi-Fi Access Points

Yilu Dong[*], Tianchang Yang[*], Nathaniel Bennett[†‡], Arupjyoti Bhuyan[†], and Syed Rafiul Hussain[*]
[*]Department of Computer Science and Engineering, The Pennsylvania State University, University Park, PA, USA
[†]INL Wireless Communication Research, Idaho National Laboratory, Idaho Falls, ID, USA
[‡]Florida Institute for Cybersecurity Research, University of Florida, Gainesville, FL, USA
yiludong@psu.edu, tzy5088@psu.edu, bennett.n@ufl.edu, arupjyoti.bhuyan@inl.gov, hussain1@psu.edu

***Abstract*—The Automated Frequency Coordination (AFC) system enables secure spectrum sharing between Standard Power Wi-Fi APs and 6 GHz incumbents. However, compromised AFC components risk causing harmful interference. In this work, we demonstrate the first practical attack against commercial Wi-Fi APs by impersonating an AFC server to inject forged *availableSpectrumInquiryResponse* messages. By exploiting flawed client-side implementations, we successfully launch targeted interference and denial-of-service (DoS) attacks within protected frequencies. Our findings underscore the critical need for a more rigorous and prescriptive AFC specification.**

***Index Terms*—Wi-Fi, Spectrum Sharing, AFC.**

I. Introduction

To address spectrum overcrowding in existing Wi-Fi bands (2.4 and 5 GHz), the Federal Communications Commission (FCC) recently opened the 6 GHz band for unlicensed consumer use [1]. However, this frequency is already occupied by existing fixed-link devices that support critical applications, such as cellular network backhaul and emergency services. Consequently, consumer 6 GHz Wi-Fi devices risk interfering with incumbents and causing service disruptions. To protect these licensed incumbents, the Automated Frequency Coordination (AFC) system was enforced. This system prevents interference by calculating and assigning maximum allowable transmission powers to Standard Power (SP) Wi-Fi Access Points (APs) based on their geolocation and configuration.

Despite its critical role, the security and robustness of the AFC system remain understudied. Prior research [2], [3] on spectrum sharing has primarily focused on utilization and optimization, with little regard for security in protocol design and implementation. While one recent study [4] demonstrated that an external attacker could manipulate AP-reported data (e.g., geolocation) to influence server-side AFC calculations and cause interference, it operates under the assumption that the attacker cannot alter the AP's internal configurations. Another work [5] explored potential attacks between the AFC client and server, but the proposed vulnerabilities remain conceptual and high-level. Consequently, neither of these studies provides an in-depth analysis of real-world AFC clients.

To bridge this gap, we investigate AFC clients running on two different commercial 6 GHz Wi-Fi APs. We impersonate an AFC server, demonstrating the capability to launch forced channel selection and denial-of-service (DoS) attacks. Ultimately, our work uncovers practical, real-world implementation flaws and highlights the urgent need for standardized security practices to ensure a robust spectrum sharing ecosystem.

In summary, our key contributions are:

- We systematically analyze AFC clients on two commercial Wi-Fi APs to identify practical exploits.
- We develop a framework to inject forged *availableSpectrumInquiryResponse* messages, successfully launching forced channel selection and DoS attacks in commercial standard power 6 GHz APs.
- We propose concrete mitigations vendors should implement to address the discovered vulnerabilities.

II. The AFC System

The introduction of Wi-Fi 6E [6] allows Standard Power (SP) Access Points (hereafter simply APs) to transmit at high power (up to 36 dBm EIRP) in the 6 GHz band, posing a direct interference risk to critical Fixed Service (FS) incumbents [7]. While passive interference has been studied [8], the active weaponization of these APs remains unexplored. To prevent harmful interference

This work is supported by a research grant from the Department of Energy (DOE) Office of the Cybersecurity, Energy Security, and Emergency Response (CESER).

and maintain an interference-to-noise ratio (I/N) strictly below -6 dB, the FCC mandates that APs coordinate with a cloud-based AFC system [9]. As illustrated in Figure 1, an AP initiates this process by sending an *availableSpectrumInquiryRequest* containing its location and device parameters. The AFC server then evaluates nearby incumbents using regulatory databases and dictates permitted channels and transmit powers via an *availableSpectrumInquiryResponse*.

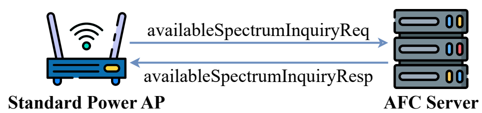

Fig. 1: AFC System Architecture

III. Threat Analysis

In this work, we consider an attacker with direct access to a commercial standard power AP who attempts to bypass AFC controls to operate at arbitrary power levels, potentially causing harmful interference to incumbent services in the 6 GHz band.

A. AFC Server Impersonation

The AFC specification [10] mandates encrypted and integrity-protected communication between the AFC client and the server. In practice, this requirement is achieved using Transport Layer Security (TLS). While TLS is the standard for securing communication and is cryptographically secure, error-prone implementations can still render the system vulnerable [11]. By exploiting implementation-level flaws, an attacker may hijack the legitimate connection between the AFC client and the server. Instead of contacting the authentic AFC server, the traffic is redirected to an attacker-controlled server, as illustrated in Figure 2.

B. AFC Response Forgery

Once the AFC server is compromised or impersonated, the attacker intercepts the *availableSpectrumInquiryRequest* and provides a forged *availableSpectrumInquiryResponse* to the client. The *availableSpectrumInquiryRequest* contains sensitive information, such as the AP's current geolocation, allowing the attacker to track connected APs.

More harmfully, the attacker can manipulate the *availableSpectrumInquiryResponse*, which provides the available frequencies and channels permitted for the AP. By forging this message, the attacker gains the capability to: ❶ force the AP to transmit on a specific set of

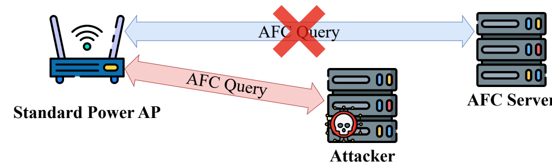

Fig. 2: Attacker Impersonating the AFC Server

frequencies and channels; ❷ control the maximum transmission power of the AP; and ❸ completely disable 6 GHz transmission. These capabilities enable targeted interference against incumbents operating in the 6 GHz band by actively setting overlapping channels and maximum transmission powers, as well as denial-of-service (DoS) attacks against 6 GHz Wi-Fi users. To maximize the likelihood of successful interference, an attacker can strategically target APs located near known FS links by querying the public FCC Universal Licensing System (ULS) database. We demonstrate this forced channel selection attack on commercial-off-the-shelf (COTS) APs in the following section.

IV. Attacks on Access Points

We evaluate the AFC clients on 2 commercial-off-the-shelf (COTS) APs: the Ubiquiti U7 Pro Outdoor [12] and the ASUS GS-BE18000 [13].

A. Implementations of AFC AP

Both evaluated APs run Linux-based operating systems and provide users with shell access for device management. The AFC client on both devices is compiled as an executable ELF program. To secure communication with the AFC server, the U7 Pro Outdoor implements standard TLS, requiring the AP to verify the server's certificate. The GS-BE18000 provides stricter security by implementing mutual TLS (mTLS), where both the server and the client cryptographically verify each other, significantly raising the bar for Machine-in-the-Middle (MitM) attacks.

Despite utilizing TLS, the U7 Pro Outdoor verifies the server's identity using the OS-level certificate store located at /etc/ssl/certs/ca-certificates.crt. This file can be modified by any user with SSH access. In contrast, the GS-BE18000 mitigates this risk through certificate pinning [14], utilizing a read-only, dedicated certificate exclusively for verifying the AFC server. We summarize these implementation differences in Table I.

B. Inject AFC Response

The editable OS-level certificate store in the U7 Pro Outdoor presents a critical vulnerability. In real-world

Device	Shell Access	Security Protocol	Certificate Pinning
U7 Pro Outdoor	Yes	TLS	No
ASUS GS-BE18000	Yes	mTLS	Yes

TABLE I: Comparison between Tested Devices

enterprise or residential deployments, network devices frequently suffer from weak, default, or previously compromised management credentials. A local network adversary can exploit these weak credentials to gain SSH access to the AP. Then, the adversary modifies the CA configuration and executes DNS spoofing to hijack traffic destined for the AFC server.

To demonstrate this exploit, we generate a self-signed root CA and install it into the AP's trust store. We then deploy a framework to automatically issue valid-looking certificates for the domains the AP attempts to contact. This establishes a MitM proxy capable of monitoring and intercepting all traffic between the AP and the internet. Consequently, we gain the capability to block AFC traffic entirely, which causes the AP to disable its 6 GHz radio, as shown in Figure 3.

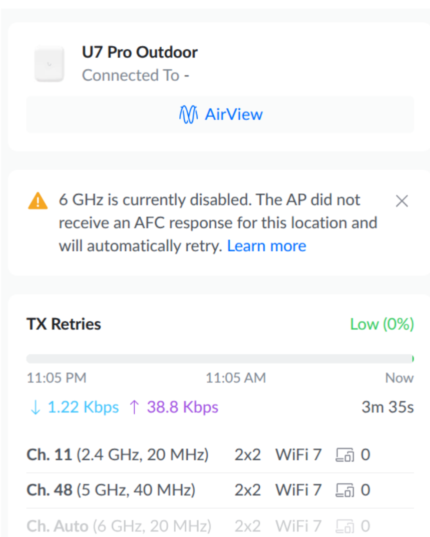

Fig. 3: AP with No AFC Response

We inject our crafted AFC response by intercepting the *availableSpectrumInquiryRequest* destined for the AFC server endpoint. To form a valid response that the client will accept, we mirror the AP's `requestId` and set the `availabilityExpireTime` to 24 hours after the request time.

C. Force Channel Selection

Once our MitM infrastructure is established, we inject crafted AFC responses into the Ubiquiti AP. As shown in Listing 1, we restrict the available spectrum by providing only a single channel (181) and 20 MHz of bandwidth to the AP. Upon receiving and validating this crafted response, the AP forcefully migrates its transmission to our attacker-specified channel (shown in Figure 4).

Recent work by Bennett et al. [5] hypothesizes that a compromised AFC server could send an *availableSpectrumInquiryResponse* specifying frequencies outside the AP's requested range, effectively forcing the AP to operate on prohibited channels. To evaluate this attack vector, we probed the client's validation mechanisms by supplying the AP with frequencies from the U-NII-6 and U-NII-8 bands, which are legally prohibited for Standard Power APs in the United States. During these tests, the AP correctly rejects the invalid regulatory responses and re-initiates queries to the server, indicating that despite a compromised transport layer, the client preserves essential regulatory boundary checks.

```
{
  "version": "1.4",
  "availableSpectrumInquiryResponses": [{
    "requestId": "2483720664",
    "response": {
      "responseCode": 0,
      "shortDescription": "Success"
    },
    "rulesetId": "US_47_CFR_PART_15_SUBPART_E",
    "availableFrequencyInfo": [{
      "frequencyRange": {
        "lowFrequency": 6845,
        "highFrequency": 6865
      },
      "maxPsd": 23
    }],
    "availableChannelInfo": [{
      "globalOperatingClass": 131,
      "channelCfi": [181],
      "maxEirp": [36.0]
    }],
    "availabilityExpireTime": "2025-10-21T19:08:55Z"
  }]
}
```

Listing 1: Forged Response with 1 available channel

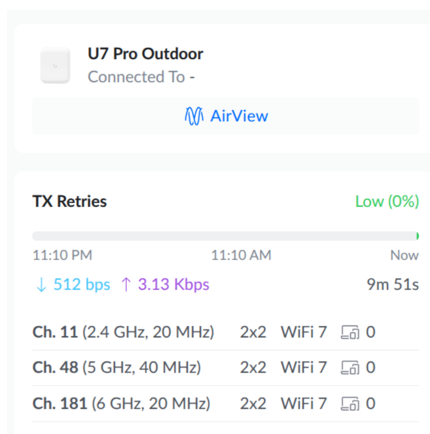

Fig. 4: Channel Selected after the Attack

V. Discussions

A. Limitations

In our attack, we assume the attacker has local or administrative access to the AP, including the capability to read and write the AP's file system. Network-level protections, such as firewalls or strict access control policies, could help mitigate this. In addition, the interference attack requires a vulnerable AP to be physically located near a protected incumbent.

B. Mitigation

To enhance the robustness of the AFC ecosystem, we strongly recommend that vendors implement certificate pinning [14] across all AFC clients. This ensures the AFC client on the AP can reliably verify the authenticity of the AFC server, effectively rejecting attacker-injected messages. Furthermore, the official AFC specification should be expanded to include concrete implementation best practices. The current version outlines high-level security concepts but lacks granular implementation details, creating ambiguity subject to vendor interpretation, inevitably introducing security risks.

C. Future Work

The security landscape of AFC systems remains largely underexplored. Because successful attacks on these systems can lead to harmful interference with incumbents and large-scale DoS, rigorous testing of both AFC client and server implementations is imperative. Future work should expand this evaluation to a wider array of commercial 6 GHz SP AP models to better understand the extent of client-side weaknesses. Additionally, analyzing widely adopted server-side references like OpenAFC [15] is critical. Applying automated vulnerability discovery techniques, such as fuzzing, to both client and server implementations will significantly enhance ecosystem resilience and pave the way for more secure spectrum sharing.

VI. Conclusion

AFC systems are fundamental to enabling efficient spectrum sharing between 6 GHz Wi-Fi devices and incumbent operators. However, their overall integrity relies heavily on the secure implementation of APs. Our research demonstrates that practical implementation flaws can prevent these systems from operating as intended, ultimately leading to harmful interference and large-scale DoS attacks. To harden these critical deployments, further security research is essential, alongside the development of a more prescriptive specification that equips AFC vendors with definitive security best practices.

References

[1] 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," Federal Communications Commission, Tech. Rep. FCC 20-51, apr 2020, 35 FCC Rcd 3852.

[2] A. Bhuyan, M. Xi, X. Zhang, S. Kasera, and S. Sarkar, "Secure mmwave spectrum sharing with autonomous beam scheduling for 5g and beyond," Idaho National Laboratory (INL), Idaho Falls, ID (United States), Tech. Rep., 2022.

[3] J. Hu, S. K. Moorthy, A. Harindranath, Z. Zhang, Z. Zhao, N. Mastronarde, E. S. Bentley, S. Pudlewski, and Z. Guan, "A mobility-resilient spectrum sharing framework for operating wireless uavs in the 6 ghz band," *IEEE/ACM Transactions on Networking*, vol. 31, no. 6, pp. 3128–3142, 2023.

[4] Y. Dong, T. Yang, A. Bhuyan, and S. R. Hussain, "GPS spoofing attacks on automated frequency coordination system in Wi-Fi 6E and beyond," in *European Wireless 2025 (EW 2025)*, Sophia-Antipolis, France, 2025.

[5] N. Bennett, A. Bhuyan, and N. J. Kaminski, "On the security of 6 ghz automated frequency coordination (afc)," in *Workshop on Security and Privacy of Next-Generation Networks (FutureG) 2026*, 2026.

[6] 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," IEEE, Tech. Rep. IEEE Std 802.11ax-2021, feb 2021.

[7] "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.

[8] S. Dogan-Tusha, A. Tusha, M. I. Rochman, H. Nasiri, J. R. Palathinkal, M. Atkins, and M. Ghosh, "Evaluation of indoor/outdoor sharing in the unlicensed 6 ghz band," in *2025 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*. IEEE, 2025, pp. 1–9.

[9] "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.

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

[11] M. Georgiev, S. Iyengar, S. Jana, R. Anubhai, D. Boneh, and V. Shmatikov, "The most dangerous code in the world: validating ssl certificates in non-browser software," in *Proceedings of the 2012 ACM conference on Computer and communications security*, 2012, pp. 38–49.

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

[13] "Rog strix gs-be18000 — networking — rog global," https://rog.asus.com/networking/rog-strix-gs-be18000/, accessed: 2026-01-23.

[14] D. Diaz-Sanchez, A. Marín-Lopez, F. A. Mendoza, P. A. Cabarcos, and R. S. Sherratt, "Tls/pki challenges and certificate pinning techniques for iot and m2m secure communications," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3502–3531, 2019.

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