On the Security of 6 GHz Automated Frequency Coordination (AFC)

Nathaniel Bennett*†, Arupjyoti Bhuyan*, Nicholas J. Kaminski*
*Idaho National Laboratory
{nathaniel.bennett, nicholas.kaminski, arupjyoti.bhuyan}@inl.gov
†University of Florida
bennett.n@ufl.edu

***Abstract*—Within the past five years, countries globally have opened 6 GHz spectrum for Wi-Fi use to account for increased throughput demand. In order to safeguard incumbent services from interference, several countries have evaluated and adopted Automated Frequency Coordination (AFC) systems; such systems calculate and relay safe operating channels and power levels to devices based on their reported location. However, the recent design and deployment of these systems combined with the inherent trust relationships introduced (control over potentially hundreds of thousands of Wi-Fi device frequency/power decisions) points to a need to rigorously evaluate the security of AFC system design. In this work, we perform a holistic security analysis of the Wi-Fi Alliance AFC standards, comprising the AFC System Reference Model and the AFC System to AFC Device Interface Specification. We consider key security properties necessary for correct AFC operation in adversarial conditions, identify several gaps in specifications that undermine these properties, and point to vulnerabilities stemming from these specification weaknesses. Our analysis reveals five findings corresponding to seven vulnerabilities, including trivial authorization bypass weaknesses, practical resource exhaustion attacks and persistent poisoning of local AFC system data stores. Our discoveries underscore the need for spectrum-sharing systems to account for a variety of potentially malicious interactions in protocol design.**

I. Introduction

Automated Frequency Coordination (AFC) systems coordinate the open use of 6 GHz frequencies by Wi-Fi devices, specifically protecting legacy "incumbent" services from harmful interference while maximizing use of available spectrum at higher power levels. AFC is one of the most recent additions to the more general trend of opening up existing bands for dynamic use; it has received significant attention and has already been evaluated/adopted for widescale use in several countries [1]–[4]. Despite the introduction of higher-risk trust relationships by such systems (e.g., the ability to influence all 6 GHz spectrum/power allocations within a given geographic location), no systematic security analysis of AFC protocols has yet been considered in academic literature.

Workshop on Security and Privacy of Next-Generation Networks (FutureG) 2026
23 February 2026, San Diego, CA, USA
ISBN 979-8-9919276-9-7
https://dx.doi.org/10.14722/futureg.2026.23023
www.ndss-symposium.org

At surface level, AFC interactions may appear almost simplistic in nature–a single interface is specified for devices to request frequencies for an area and receive appropriate power levels to operate on. However, such a view masks a number of underlying requirements that complicate operation. For instance, AFC systems must regularly update relevant licensed and barred device information, as well as geospatial measurements, from several remote data sources. Device requests are given significant flexibility in provided location bounds, uncertainty intervals and frequency ranges; in practice, servers must dynamically calculate responses over upwards of hundreds of gigabytes of sparse geospatial data. Furthermore, AFC systems are mandated to provide non-repudiatable logging and sufficiently authenticate clients it receives spectrum requests from. When the security assumptions of these requirements are violated, an adversary may gain significant attack capabilities.

Our work holisticlly analyzes key security properties necessary for AFC operation in the presence of varying threat models to identify protocol-wide vulnerabilities. We make the following contributions:

1) **Identification of Key Security Properties.** To assess the security of AFC, we first extract key security properties between the client, AFC system and National Regulatory Authority (NRA) database that are specified and/or implied by the AFC protocol. We then use these to assess interactions between the above for potential violations of those properties.
2) **Protocol Analysis of the AFC Specification.** We uncover five design weaknesses in the AFC specification that enable an adversary to carry out various attacks against devices, AFC systems, or even incumbent services across the 6 GHz band. These attacks include authentication bypass, forgery of non-repudiated log records, response poisoning via colliding cached requests, and persistent data poisoning of the AFC system's internal store of incumbent devices.
3) **Recommendations for Remediating Root Causes.** For each finding, we outline relevant portions of AFC design that lead to vulnerabilities. We subsequently provide recommended additions or alterations to the specification that would fix the underlying weakness and remediate resulting vulnerabilities. We perform responsible disclo-

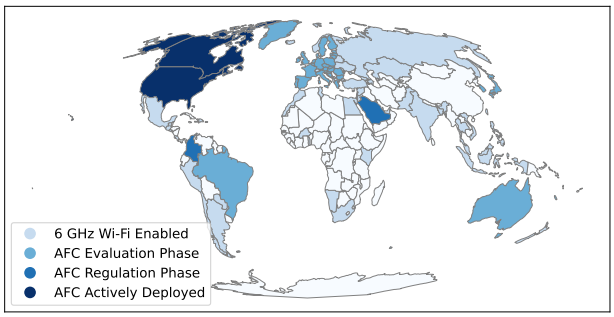

Fig. 1. Global 6 GHz Wi-Fi/AFC system adoption [5], [6]. All shaded regions permit some Wi-Fi use in portions of the 6 GHz spectrum ("Enabled"). Of these, several additional regions (including the EU) are actively evaluating test AFC deployments ("Evaluation"); Colombia and Saudi Arabia have regulatory frameworks proposed for AFC systems ("Regulation"); Canada and USA have licensed AFC systems in operation ("Deployed");

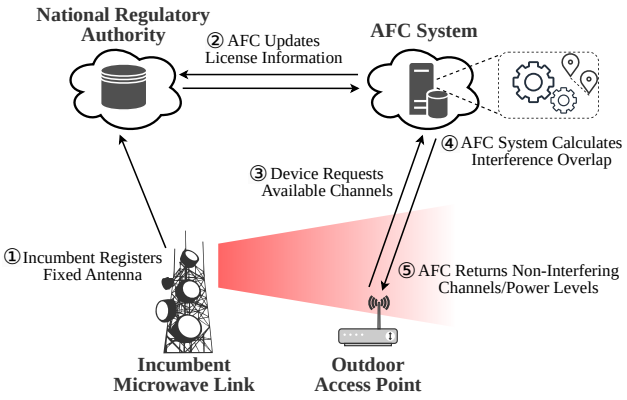

Fig. 2. Operational steps of 6 GHz Automated Frequency Coordination. Fixed microwave services are registered with the NRA on specific frequency ranges prior to operation (1). The AFC system fetches daily updates from the NRA on newly registered/deregistered services (2). Fixed Wi-Fi APs operating either outdoors or at standard power request channels to broadcast on (3); the AFC calculates the power reduction needed to avoid interference with any incumbents within range of the device (4) and returns safe operating powers for channels to the device (5).

sure of our work with the Wi-Fi Alliance and are in discussions on mitigations with members of the Wireless Innovation Forum (WInnForum).

Organization: The remainder of this paper is structured as follows: Section II describes AFC system design; Section III identifies relevant security properties/attack vectors; Section IV covers device-to-system attacks; Section V covers system-to-device attacks; Section VI covers AFC system data supply chain attacks; Section VII provides discussion; Section VIII explores related work in AFC systems and protocol analysis; and Section IX offers concluding remarks.

II. Background

A. Automated Frequency Coordination Design Goals

AFC was designed specifically to enable higher-power Wi-Fi communications over 6 GHz spectrum. Though many countries have enabled Wi-Fi use in portions or all of the 6 GHz spectrum (see colored regions of Figure 1), nearly all restrict Access Points (APs) to operate only indoors and at low power–from 23 to 30 dBm depending on region. Outdoor APs are further restricted to just 14 dBm, thereby severely limiting the range and utility of this spectrum for outdoor or high-congestion use cases. For reference, 2.4 GHz and 5 GHz are permitted in many countries for up to 36 dBm [7], more than 150x the power output of outdoor AP limits for 6 GHz. Spectrum sharing for 6 GHz spectrum was thus implemented to enable full-power operation.

Unlike other shared bands, substantial portions of the 6 GHz spectrum are allocated exclusively to fixed-position services. These services are primarily composed of high-throughput point-to-point microwave links that convey time-sensitive data across significant distances within line-of-sight [8]. Communications conveyed through these links include cellular network backhaul, power grid command and control, measurement and control of remote oil/gas pipelines, cable television relay, and railroad control signalling. Apart from point-to-point links, specific portions of 6 GHz spectrum are also allocated for Fixed Satellite Service (FSS) uplink C-band communications and for radio astronomy observations [8].

The absence of mobile services enables a more flexible, minimal design of AFC than is the case in other shared spectrum. Other sharing systems such as Citizens Broadband Radio Service (CBRS) require a persistent connection with every device using spectrum so as to direct those devices to change channels when mobile incumbents enter an area. Devices do not choose a channel; rather, they are assigned one. By contrast, AFC acts in a stateless manner–APs query once a day for the channels are available in their area, and the AFC calculates interference paths to return maximum permissible power levels for each channel back to the AP. The APs then decide what channel or channels to broadcast on based on measured interference levels, akin to Wi-Fi operation in other bands. On the back end, AFC systems update their database of registered incumbent devices each day with the designated NRA for the country the AFC is servicing to ensure any newly inserted or removed towers are updated. This full process is depicted in Figure 2.

B. AFC Specification

In partnership with the WInnForum, the Wi-Fi Alliance has specified AFC system operation through a series of design standards. These include the AFC System Reference Model [9] and the AFC System to AFC Device Interface Specification [10], as well as testing/compliance plans and test vectors [11]. While government regulation does not specifically mandate the use of these standards in developing AFC systems, all conditionally-approved and approved AFC systems to date follow the Wi-Fi Alliance AFC system to AFC device protocol specification [12]. Moreover, the FCC specifically references the Wi-Fi Alliance specifications with regards to both expected input format from devices and

TABLE I
OPERATIONAL REQUIREMENTS OF AFC SYSTEMS AND CORRESPONDING SECURITY ATTRIBUTES.

Security Attribute	Description	Consequence of Property Violation
Incumbent Availability (**P1**)	Incumbent Unimpaired by Wi-Fi Device Interference	Denial of Service of critical infrastructure links
↪ Spectrum Response Integrity	AP receives untainted, *correctly-calculated* response	Adversarially-crafted Spectrum Responses
↪ NRA Update Integrity	AFC System receives untainted/up-to-date incumbent info	Bogus incumbents added, legitimate ones removed from calculations; adversarial channel selection
Device Availability (**P2**)	AP operable in 6 GHz spectrum (if applicable)	Degraded/disrupted service for Wi-Fi access
↪ AFC System Availability	AFC System returns timely responses to requests	Denial of Service of AFC servers & devices
↪ Spectrum Response Integrity	AP receives untainted, *correctly-calculated* response	Adversarially-chosen Spectrum Response fields
↪ NRA Update Integrity	AFC System receives untainted/up-to-date incumbent info	Bogus incumbents added, legitimate ones removed from calculations; adversarial channel selection
Accountability (**P3**)	AFC interactions can be audited post-event for culpability	Mis-attribution of interference; framing attacks
↪ AFC System Non-Repudiation	AFC System produces unforgeable spectrum responses	Device misdirection, framing
↪ Device Authorization	Request device identifiers originate from the correct client	Authorization bypass; cross-device impersonation
↪ Client Authentication	Client identity verified by the AFC system	Authentication bypass; under-billing

Note: $\alpha \hookrightarrow \beta$ denotes β as a prerequisite property necessary for α to hold in AFC operation.

necessary vectors for testing compliance [13]; as such, the Wi-Fi Alliance specification is the de-facto standard for all operational AFC systems.

AFC System-to-Device Protocol. The AFC System to AFC Device Protocol specification defines the `availableSpectrumInquiry` HTTP API for APs to query an AFC system for 6 GHz spectrum availability. As part of this API, the AP sends a JSON payload composed of a list of one or more `availableSpectrumInquiryRequest` objects, each of which contains identifying information for the device making the request, the approximate location and elevation of the device, and the requested frequencies and associated power levels that the device intends to receive access for. Both the location and elevation of the device are defined in terms of uncertainty areas, as APs often ascertain location from GPS services that can have significant variation in precision. Requested spectrum is indicated via one or both of an `inquiredFrequencyRange` and `inquiredChannels` fields, which respectively contain *lists* of frequency ranges and channel sets. Desired power level is indicated by an optional `minDesiredPower` field.

Upon receiving such a request, the AFC system considers all incumbent services operating within a given region (often a range upwards of 200km [14]) and calculates the maximum operating power that will still result in less than a certain threshold of interference. When the location reported by the AP has uncertainty bounds, the AFC system identifies the region within the AP's three-dimensional uncertainty bound that has the lowest maximum operating power and returns it. This process is repeated for each requested channel or frequency band. Once completed, the AFC system returns an `availableSpectrumInquiry` response that includes an expiration time and lists of available channels/frequency bands with associated maximum power levels for each.

Term Disambiguation. to avoid reader confusion, this paper will hereafter refer to an `availableSpectrumInquiry` Request simply as a "Spectrum Request" in subsequent text, whereas the `availableSpectrumInquiry` Request Message (the JSON payload of the inquiry that contains one or more Spectrum Requests) will be referred to as an "Aggregate Request Message". Likewise, the `availableSpectrumInquiry` Response will hereafter be referred to as a "Spectrum Response", while the `availableSpectrumInquiry` Response Message (which contains one or more Spectrum Responses) will be referred to as an "Aggregate Response Message".

III. AFC SECURITY ATTRIBUTES

A. AFC Operational Requirements

To ensure that we consider vulnerabilities that pose meaningful risks, we first identify two base properties that *must* be upheld to ensure correct AFC system operation:

1. An AP should not receive channels or power levels from the AFC system that would cause it to interfere with an incumbent device.

In practice, whether a device will cause interference is determined by predefined algorithms for approximating radio interference in combination with geospatial data for the region in question. An AFC system is considered to be suitably operating so long as the frequency allocations it returns to APs adheres to those algorithms. Fundamentally, this operational requirement helps to ensure the security property of incumbent availability, which we denote as **P1** in Table I.

2. An AP should receive approval from the AFC system to operate on channels/power levels that would not result in incumbent interference.

APs are mandated to request and obtain approval from an AFC system before transmitting wirelessly in the 6 GHz spectrum. As such, an AFC system that is unresponsive or otherwise returns incorrectly-restricted responses will lead to degraded service on querying APs. We denote this as **P2** in Table I.

Beyond operational requirements, the AFC protocol specifies logging of requests/responses for non-repudiation purposes as part of operation. Non-repudiation is of particular importance in the context of frequency spectrum allocation,

as wireless interference is subject to federal regulation and significant fines or prosecution in most jurisdictions. In such cases, distinguishing between illegal AP operation or incorrect AFC system responses as the cause of interference becomes of critical importance. Denoted as **P3** in Table I, we define this property as:

3. Logged requests/responses should be able to ensure accountability in the event of wireless interference events.

B. Associated Security Properties

From these three operational requirements, we explore the security properties that must be upheld for an AFC system to correctly operate. Table I shows identified security properties and their relation to foundational operational requirements.

Having considered security attributes through the various interactions of AFC protocol operation, we now characterize specification weaknesses that violate one or more of the above requirements. We identify five such specification weaknesses corresponding to seven vulnerabilities under three separate threat models, which we describe hereafter.

IV. Device-to-System Threats

We first consider design weaknesses in the AFC specification that may enhance the attack capabilities of an adversarially-controlled AP. Attacks stemming from these weaknesses generally take the form of a device sending one or more specially-crafted Spectrum Requests to elicit undesirable behavior.

a) Threat Model: We consider an adversary that has obtained credentials to communicate with an AFC system for a single device. Such devices are available for retail purchase; an adversary may thus extract keys from memory after acquiring such a device. The adversary's Device ID may be blacklisted–in other words, any request to an AFC server by the device should correctly authenticate but return error `101 DEVICE_DISALLOWED`. We consider only the `availableSpectrumInquiry` API, as all other APIs are designated as vendor-specific extensions.

A. Authentication Uncoupled from Device ID Authorization (Finding 1)

Although the AFC System Reference Model leaves the specific means of authenticating client devices up to implementation, it does mandate some form of client authentication for each incoming request. As such, authentication procedures are performed via some data medium other than the payload containing each Spectrum Request. A consequence of this is that the device identifier field contained in each Spectrum Request within the payload is not tightly coupled with authentication procedures. While the specification indicates that the Device Responder Function is also responsible for *validating* the syntactic correctness of JSON fields, it does not require *verifying* that the Device ID passed in each Spectrum Request of the payload actually corresponds to the authenticated client sending the HTTP request. Indeed, any device non-blacklisted identifier that corresponds to a registered device may readily

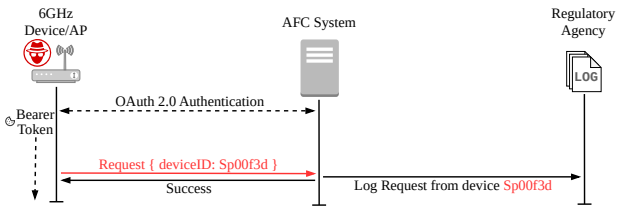

Fig. 3. AFC Server Device Identifier Authorization Bypass

be considered both syntactically and semantically valid by the system; ensuring the communicating client is authorized to use that device identifier is a separate matter.

As a consequence of this discrepancy, a conforming AFC server may readily accept requests containing arbitrary device identifiers, so long as the client has first successfully authenticated with the system (shown in Figure 3). Moreover, while obtaining a valid device identifier involves strict government-regulated processes, the only barrier for an adversary obtaining client credentials to an AFC system is to become a paying customer of that service or to purchase an AP with such a license. We identify three potential vulnerabilities stemming from this design weakness that an adversary would not otherwise have the capability of carrying out; we describe these subsequently.

VULN-1 - Device Enumeration: An AFC device may enumerate valid, invalid and blacklisted device identifiers by sending sequential requests from various spoofed device identifiers.

The device identifier is composed of the manufacturer's unique Serial Number in combination with a government Certification ID number for the device model (such as an FCC ID, as depicted). These two numbers uniquely identify a device or AP. Although both of these sub-identifiers may be upwards of a dozen characters in length, Serial Numbers are commonly assigned incrementally, with many of the digits remaining static for a given product. Given an oracle to check whether a serial number is correct, an attacker may need to guess only four to seven digits provided they know the device model of a target. On the other hand, Certification IDs–such as the FCC ID in the US or the IC-ID in Canada–are published openly online and include associated device and manufacturer information [15], [16], making them trivially discoverable.

The practical outcome of these conditions is that an attacker may readily discover and enumerate devices that are authorized for (or blocked from) operation by incrementally checking spoofed device Serial Numbers along with a spoofed valid Certification ID against the AFC system. When coupled with the fact that an Aggregate Request can validly contain thousands of Spectrum Requests with distinct identifiers, an attacker may reasonably succeed at harvesting device identifiers via repeated Aggregate Requests. This knowledge may then be used to carry out subsequent device-specific attacks.

VULN-2 - Blacklist Bypass: An AFC device may bypass

device identifier authorization to elicit and receive successful AFC system responses, even when the device would otherwise be banned.

The AFC specifications mandate that devices barred by the NRA have their Spectrum Requests be rejected. The AFC system queries the NRA for a list of such disallowed devices to block from operation. In the event that an adversary-controlled device is added to this list, the adversary may continue to query for Spectrum Responses and carry out attacks by changing its Device ID to a known permitted Device ID. A valid device identifier may be obtained by the adversary either exploiting **VULN-1** or through external knowledge.

VULN-3 - Device ID Masquerading: An AFC device may trivially spoof any other device when making Spectrum Requests without needing that device's authentication credentials.

An adversary can carry out this attack by first authenticating with the AFC under whatever authentication scheme the AFC has implemented (e.g., mutual TLS), then send Spectrum Requests with a Device ID corresponding to a target victim AFC device. Furthermore, AFC system specifications do not include any mechanism for coupling individual Spectrum Requests to authenticated session credentials during logging; as such, only the device identifier may be included as part of the logged Spectrum Request. A compromise in device authorization may therefore result in violation of non-repudiation requirements for AFC logging, as described in the following scenario. An adversarial device may persistently send overtly malicious Spectrum Requests from a chosen victim's Device ID as part of an attack on the AFC system to successfully frame a victim device (e.g., a device operator or manufacturer) as the originator of the attack. Upon detection of non-conforming broadcasts in an area or suspicious incoming activity on the AFC system, non-repudiated logs would point to the victim as the perpetrator of the illegal behavior, with no indication of the adversary's involvement.

Remediation: To prevent authorization bypass, the AFC specification should require that implementations verify Device IDs to ensure they correctly correspond to provided client credentials and reject improper Device IDs for a client. We emphasize that checks must be carried out *for every Spectrum Request in the Aggregate Request Message*, as each Spectrum Request may contain a distinct device identifier; checking only one of the requests would be insufficient. To adapt to this requirement, AFC system implementations would need to store and keep track of device (`identifier`, `client`) credential mappings in the Internal Database Function. This may reasonably be achieved by having subscribers provide the serial number of a given device credentials are being provisioned for at the time of registration and then permitting only that serial number to be used for that particular set of credentials. Such a system could also be adapted to handling a batch of permitted serial numbers where proxying occurs.

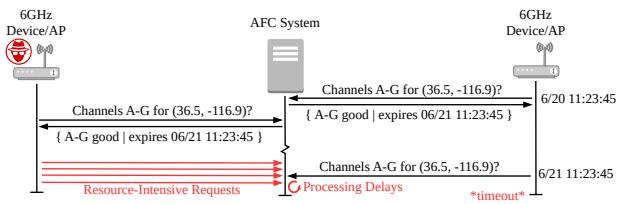

Fig. 4. Targeted Device Denial-of-Service Attack

B. Under-Constrained Request Fields (Finding 2)

The AFC system-to-device protocol specification not only describes the format of protocol data fields to be exchanged between device and server, but also provides restrictions on value ranges within those fields. However, we identify several instances of underspecified or unspecified field restrictions that enable an adversarial device to significantly increase the resource consumption of a given Aggregate Request Message:

Spectrum Request cardinality: As mentioned in Section II, each Aggregate Request is specified to contain one or more Spectrum Requests from various downstream devices. However, the specification makes no limit on the number of Spectrum Requests contained, and the total size of such an Aggregate Request is likewise left unconstrained in the standard.

Frequency-related fields: Each Spectrum Request may either contain a list of frequency ranges, a list of `Channels` objects, or both. These frequency and channel ranges are not required to be unique/nonoverlapping at any point in the standard, and `Channels` objects themselves contain sets of potentially duplicate channels. No maximum number of channels or frequency ranges is specified.

Location-related fields: A Spectrum Request must include exactly one of three possible means of identifying location– either an Ellipse object, a Radial Polygon, or a Linear Polygon. Both Linear and Radial Polygons are restricted to between three and 15 points/vertices respectively, with the length between each point not exceeding 120 kilometers– permissive enough to accept a device location uncertainty region of *more than 250 square kilometers*. Ellipse objects have no specified restrictions on the maximum length of their major/minor axes. As frequency interference calculations are often nonlinear, every arcsecond (30x30 meter square) area within the uncertainty region must separately be assessed to fulfill such a request.

Elevation-related fields: AP elevation is considered in AFC standards when calculating line-of-sight interference. A device may report its height in terms of meters Above Ground Level (AGL); when used, the AFC system must recalculate height for every arcsecond area and factor it into interference calculations. Furthermore, Spectrum Requests send a height uncertainty field which can result in multiple calculations per each arcsecond coordinate area.

The above four behaviors lead to the following vulnerability:

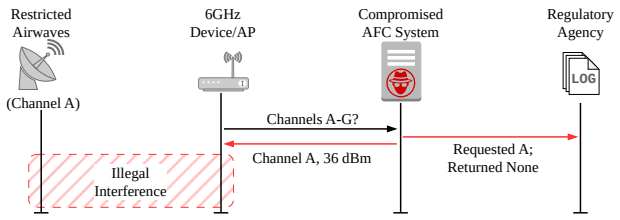

Fig. 5. Non-Repudiated Log Forgery Attack

VULN-4 - AFC Server Resource Exhaustion DoS: An AFC device may craft requests specially designed to require the AFC system to repeatedly process tens or even hundreds of gigabytes of geospatial data files.

We observe that an incoming request may be designed to force a number of repeated recalculations of frequency/channel availability that can quickly grow untenable, potentially incurring upwards of 100x increases in request processing CPU time. Individual calculations may be for a selected frequency that maximizes work performed by the AFC server, and are proportional to the product of the number of Spectrum Requests contained within the message, the number of frequency/Channel objects, and the number of channels within each Channel object. In practice, AFC servers store and process upwards of hundreds of gigabytes of geospatial data to be queried and transformed for each request component, resulting in significant and memory constraints computational effort on the order of minutes of CPU time *per Spectrum Request*. When further compounded by an adversary that can send hundreds of Spectrum Requests within a single Aggregate Request, an adversary could quickly overwhelm even a well-provisioned server.

Remediation: The AFC specification should include hard limits on the number of Spectrum Requests permitted per Aggregate Request, require channels and frequencies not repeat or overlap within a single request. The specification should also restrict the currently relaxed limit on location uncertainty bounds to ensure resource requirements cannot be scaled up quartically by an adversary. AFC operators may make system-specific mitigations as well, such as rate-limiting the amount of CPU processing time a given client (as identified by authentication credentials) is permitted before requests are throttled.

V. AFC System-to-Device Threats

Our second attack scenario considers attacks an adversary that has temporarily compromised an AFC system may be capable of. This requires much stronger prerequisites than our first scenario, necessitating some independent vulnerability on the AFC system that an adversary compromises. We note that channel selection and transmission power decisions for Spectrum Responses are fundamental to this capability; to wit, a controlled AFC can force devices to use particular frequencies within the range of those requested, or deny access to services. As such, our focus is instead on enhanced capabilities made possible to the adversary specifically due to design weaknesses in the AFC specification that go beyond such an attack.

Threat Model: In the following findings, we consider an adversary that has obtained temporary access to the operation of one or more AFC system deployments. The adversary can manipulate the outputs of the AFC system, such as the contents of Spectrum Responses returned to AFC devices or reported logs.

A. Unsigned Device Requests (Finding 4)

Though the AFC specifications describe non-repudiation as a goal of logging functions in the AFC system, no mechanism is specified to bind logged requests to authenticated sessions. An AFC system implementation carrying out logging of only the request/response payload is prone to spoofed or overwritten logs being undetected due to the payloads having no integrity protection mechanisms.

VULN-6 - Arbitrary Non-Repudiated Log Forgery: Following from **VULN-3**, the compromised AFC device may additionally send crafted response logs to a reporting agency for each request appearing to return legitimate values.

Remediation: Specify an integrity mechanism such as HTTP Request Signing (RFC 9421) as part of client authentication, and mandate server logging of HTTP signatures/payloads for each request.

B. Unconstrained Responses (Finding 5)

During normal operation, the AP queries for a chosen set of frequencies and/or channels to receive spectrum allocation decisions for from an AFC system. However, the AFC protocol specification never specifies that responded frequencies or channels must strictly be within the set requested–or even within the permitted frequency bands of the country of operation. As different countries permit different portions of 6 GHz spectrum (arising in part from distinct incumbent concerns), routers commonly implement all 6 GHz and subsequently enable communication on specific frequencies returned by the AFC response. Although a router may be configured for a certain country and only request channels permitted by that country, a compromised AFC may direct it to operate entirely out of permissible bands, leading to the following vulnerability:

VULN-7 - Out-of-Range Targeted Frequency Congestion: A compromised AFC server may return only a targeted frequency/channel to all requests coming from a specific area, even when the target frequency lies outside the requested range or outside of allowed bands. This enables it to oversaturate that channel and degrade service for any incumbent devices when APs automatically work based off Spectrum Response values without cross-validating requested channel ranges. This is *in spite of* any conservatively-scoped requests made by access points, as responses may exist outside of request fields.

Remediation: The AFC specification should mandate that AFC server response frequencies must be within the range of

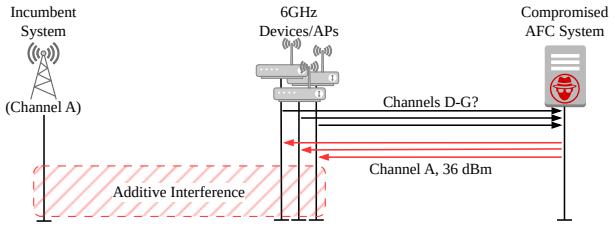

Fig. 6. Targeted Frequency Congestion Attack against Incumbents

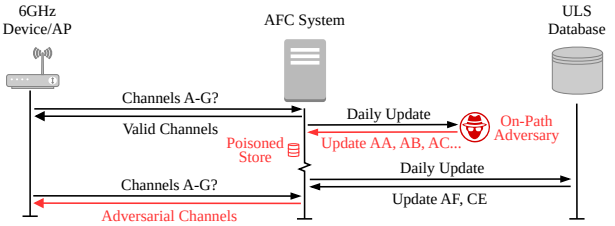

Fig. 7. AFC Internal Data Store Poisoning Attack

those requested and that devices should independently validate channels and frequency bands returned in Spectrum Responses to ensure appropriate transmission.

VI. NRA Update Mechanism Threats

As mentioned in Section II, AFC systems periodically refresh data on incumbent receivers and barred device IDs from the NRA database, the specific configuration of which may vary by country. Queried updates are commonly designed to enable incremental fetches of daily changes rather than re-downloading the entire database of devices. This section considers adversaries targeting the NRA Update communication path.

Threat Model: For this section, we consider an adversary that temporarily has on-path Man-in-the-Middle capabilities during the AFC's daily NRA update routine, such as through DNS cache poisoning [17], latent configuration [18] or network-layer attacks [19]. The adversary is not privy to any internal sensitive information on the data source, such as TLS keys.

A. Absent Data Transport Security (Finding 3)

Neither AFC specification requires any form of transport security for incremental NRA updates or other underlying geospatial data sources. This is in direct contrast to the AFC system-to-device protocol, which mandates TLS usage and specifies required minimum TLS versions, ciphers and verification steps (including CLR/OCSP checks). As such, an AFC system implementation in full compliance with specifications may reasonably retrieve daily Universal Licensing System (ULS) over unencrypted channels, such as via unencrypted FTP or HTTP. Similarly, no verification of data authenticity is specified–updates may be provided without any signature or hash to independently verify the data's contents. This lack of verification, when combined with the incremental approach taken for updating licensing data, leads to potentially long-lasting consequences for AFC systems, outlined in the next vulnerability:

VULN-5 - AFC Data Poisoning: An adversary may exploit weak data transport security to arbitrarily remove existing incumbents or spuriously add fake incumbents to the AFC's internal data store.

The AFC system has no mechanism to verify the authenticity of the data on arrival, so it will use readily accept adversarially-tampered data at the time of attack. Moreover, subsequent legitimate daily updates that are retrieved post-compromise provide no mechanisms for checking that past updates have not corrupted the AFC's internal data store. An attacker with brief Man-in-the-Middle access to these update channels, such as via DNS cache poisoning, can therefore alter the behavior of the AFC system indefinitely after a one-time attack, altering spectrum decisions for all devices serviced by the system until an entire refresh of the database is performed. The adversary may craft an update that spuriously removes an incumbent they wish to be interfered with while adding spoofed incumbents in the same area on all other channels, thereby directing all APs onto the channel that would interfere with the incumbent. Alternatively, the adversary may selectively deny service to 6 GHz access by region by adding spoofed incumbents to an area that would lead to calculated interference on all bands.

While we primarily focus on the on-path attacker threat model, we note this attack is similarly applicable in scenarios where the data integrity of the NRA system is compromised. The dynamic nature of incumbent license information necessitates data modification mechanisms in the server; known threats such as file upload vulnerabilities or SQL injection could enable an attacker to temporarily overwrite license information, thereby attaining the same capability as that of an on-path attacker.

Remediation: Mandate TLS for all AFC server commmunications with external source databases. For daily incremental updates, add incremental hashes so that the server can detect post-compromise if its past data has been poisoned in some way.

VII. Discussion & Future Directions

Completeness and Efficacy in Implementation. All of the identified vulnerabilities in our work are based on AFC specification weaknesses, and identified fixes are generally compatible with existing interface definitions. As this is a holistic and not formal analysis, we do not claim completeness or absence of other potential attacks. Our work does not make the claim that these deficiencies are universally or generally exploitable on any AFC implementation–a developer implementing AFC system functionality with security in mind may reasonably identify some of these flaws individually and incorporate mitigations into standard operation. Rather, our

work demonstrates that the existing specification is inherently insecure under certain threat models and that an implementation in full conformance to that specification may still be manipulated to violate key security properties of spectrum sharing. Moreover, specific attacks (such as **VULN-4**) are inevitable due to the AFC protocol specifying overly relaxed input parameter limits that an adhering implementation would use.

Fundamental System-to-Device Threats. As noted in Section V-B, the scenario of a compromised AFC system poses the threat of arbitrary manipulation of 6 GHz wireless transmission decisions for potentially millions of APs. Moreover, attacks on network routing (such as BGP hijacking or DNS cache poisoning) can enable mis-issuance of TLS credentials of routing of requests to an adversary, leading to the same outcome. While these require significant attacker prerequisites, they correspondingly offer the potential for remote wireless interference of critical infrastructure links without a physical presence–a strong capability more likely sought after by well-funded or nation-state adversaries. Our work does not identify any solution to this threat; future research may consider protocol-compatible or device-side mechanisms for mitigating the effectiveness of such a threat.

Active vs Implicit Allocation of Shared Spectrum. AFC is not the only spectrum sharing protocol in active deployment; both CBRS and Television White Space (TVWS) were considered and implemented for other frequency spectrums years prior to the adoption of AFC. One key differentiating feature between these protocols is the use of *active allocation*, wherein the coordinating database statefully leases and tracks individual device use of spectrum in regions, versus *implicit allocation*, where the database provides devices all available frequencies/powers requested and leaves the decision of which to choose up to the device. CBRS, for instance, employs an active management strategy to individual device spectrum allocations, with varying tiers of guaranteed service availability for querying devices. AFC, on the other hand, does not track device spectrum use or dynamically restrict available channels in responses based on what past devices have requested.

As a more general takeaway of our work, we note that the stateless design used by AFC surprisingly mitigates the severity of certain identified specification weaknesses. Specifically, the device masquerading attack discussed in **VULN-3** cannot be used to manipulate the resulting responses returned to the device being masqueraded, as the AFC server does not track device state and returns the same static response for any given request. Were this specification vulnerability to be uncovered in CBRS, it would grant an adversary the ability to arbitrarily and persistently deny service to any individual device using the allocation system by spoofing an already actively-managed session from that device. Furthermore, the adversary could carry out resource exhaustion of spectrum availability by spoofing allocation requests from a number of spoofed devices, including those with higher tiers of service availability guarantees, and cause over-billing of services for other users. As such, the simplicity of AFC actually protects it from more sophisticated attacks that would otherwise follow authorization bypass.

VIII. Related Work

The 6 GHz AFC protocol is a relatively recent addition to several dynamic spectrum sharing techniques, though it has the potential to be integrated with significantly more devices given its role in high-throughput Wi-Fi 6E and 7 protocols. As such, AFC protocol security is relatively unexplored, though work by Dong et al. [20] explores the threat model of GPS spoofing at the AP as a means of disrupting correct AFC operation. Apart from security-specific studies, other publications have experimentally demonstrated the potential for expanded deployment of 6 GHz AFC in regions such as South Korea [21] and Taiwan [22].

Protocols such as Spectrum Access System (SAS) for CBRS and Protocol to Access White Space (PAWS) for TVWS have received more consideration, with both general explorations of security challenges inherent to operation [23] and specific proposed revisions to the SAS protocol to introduce preservation of privacy [24]. However, the majority of research has focused on more fundamental security and availability challenges to dynamic spectrum sharing [25]. Several works propose various decentralized solutions or blockchain [26], [27], both as a means of brokering access and to attempt to provide stronger availability and integrity guarantees under the threat model of a compromised/malicious spectrum sharing provider. For the concern of spectrum misuse, Jin et al. [28] proposed a crowdsourced framework for detecting violations of spectrum licensing that operates on top of spectrum sharing systems. More recent work has explored the challenge of dynamically sub-leasing spectrum in secure and enforceable ways [29], [30].

IX. Conclusion

AFC fundamentally enables remote decisions on radio frequency use that may overlap and interfere with incumbent devices; as such, ensuring the security of such protocols is critical. Our work has identified five specification weaknesses in AFC under three adversarial models that enable a variety of vulnerabilities. We carry out responsible disclosure and report our specification flaws and corresponding proposed fixes to the Wi-Fi Alliance. Our findings point to the need for careful analysis and consideration of security in the design and implementation of spectrum sharing systems to protect both incumbent systems and services operating over dynamically-shared spectrum.

Acknowledgment

This material is based upon work supported by the U.S. Department of Energy, Office of Science, Office of Cybersecurity, Energy Security, and Emergency Response, under Award Number DE-AC07-05ID14517.

REFERENCES

[1] RCR Wireless News. (2024) FCC approves seven AFCs for 6 GHz. [Online]. Available: https://web.archive.org/web/20250616211146/https://www.rcrwireless.com/20240224/featured/fcc-approves-seven-afcs-for-6-ghz

[2] Innovation, Science and Economic Development (ISED) Canada. (2025) List of designated dynamic spectrum access system administrators (DSASAs). [Online]. Available: https://web.archive.org/web/20250616194132/https://ised-isde.canada.ca/site/certification-engineering-bureau/en/list-of-designated-dynamic-spectrum-access-system-administrators

[3] Dynamic Spectrum Alliance. (2023) Open AFC completes the approval phase and integration of technologies to facilitate innovative Wi-Fi 6E outdoor project in Brazil. [Online]. Available: https://www.dynamicspectrumalliance.org/wp-content/uploads/2023/08/Open_AFC_FINAL.pdf

[4] ——. (2024) Dsa comments to cst on "public consultation on light licensing regulations annex for the 6 GHz frequency band". [Online]. Available: https://www.dynamicspectrumalliance.org/2024/nov/DSAComments%20toCSTontheLightLicensingRegulationsforthe6GHzband.pdf

[5] Wi-Fi Alliance. (2025) Regulations enabling 6 GHz Wi-Fi. [Online]. Available: https://web.archive.org/web/20250609175355/https://www.wi-fi.org/regulations-enabling-6-ghz-wi-fi

[6] ——. (2025) Regulations enabling 6 GHz standard power Wi-Fi. [Online]. Available: https://web.archive.org/web/20250616185538/https://www.wi-fi.org/regulations-enabling-6-ghz-standard-power-wi-fi

[7] Federal Communications Commission, "Cfr 15.247: Operation within the bands 902-928 mhz, 2400-2483.5 mhz, and 5725-5850 mhz." https://www.ecfr.gov/current/title-47/chapter-I/subchapter-A/part-15/subpart-C/subject-group-ECFR2f2e5828339709e/section-15.247, 2025.

[8] ——, "Unlicensed use of the 6 ghz band: Report and order," https://docs.fcc.gov/public/attachments/FCC-20-51A1.pdf, 2025.

[9] Wi-Fi Alliance, "AFC system reference model," Tech. Rep., 2021, version 1.0. [Online]. Available: https://www.wi-fi.org/file/afc-specification-and-test-plans

[10] ——, "AFC system to AFC device interface specification," Tech. Rep., 2023, version 1.5. [Online]. Available: https://www.wi-fi.org/file/afc-specification-and-test-plans

[11] ——, "AFC system (SUT) compliance test plan," Tech. Rep., 2023, version 1.5. [Online]. Available: https://www.wi-fi.org/file/afc-specification-and-test-plans

[12] Federal Communications Commission, "DA 22-1146: OET announces conditional approval for 6 GHz band automated frequency coordination systems," https://docs.fcc.gov/public/attachments/DA-22-1146A1.pdf, 2022.

[13] ——, "DA 23-759: OET announces commencement of testing of the 6 GHz band automated frequency coordination systems," https://docs.fcc.gov/public/attachments/DA-23-759A1.pdf, 2023.

[14] MIST, "Afc and 6 ghz incumbents," https://www.mist.com/afc-and-6-ghz-incumbents/?hl=en-US#:~:text=For%20medium%20distances%20of%2030m,except%20in%20a%20few%20scenarios., 2020.

[15] Federal Communications Commission. (2025) FCC ID search. [Online]. Available: https://www.fcc.gov/oet/ea/fccid

[16] Innovation, Science and Economic Development Canada. (2025). [Online]. Available: https://ised-isde.canada.ca/site/certification-engineering-bureau/en/wireless-program/radio-equipment-list-rel

[17] K. Man, Z. Qian, Z. Wang, X. Zheng, Y. Huang, and H. Duan, "DNS cache poisoning attack reloaded: Revolutions with side channels," in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*. Association for Computing Machinery, 2020, pp. 1337–1350.

[18] E. Pauley, R. Sheatsley, B. Hoak, Q. Burke, Y. Beugin, and P. McDaniel, "Measuring and mitigating the risk of IP reuse on public clouds," in *2022 IEEE Symposium on Security and Privacy (SP)*, 2022, pp. 558–575.

[19] C. Testart, P. Richter, A. King, A. Dainotti, and D. Clark, "Profiling BGP serial hijackers: Capturing persistent misbehavior in the global routing table," in *Proceedings of the Internet Measurement Conference*. Association for Computing Machinery, 2019, pp. 420–434.

[20] 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.

[21] S. Park, B. Kim, I. Kim, and J.-B. Seo, "Deploying automated frequency coordination system for WiFi 6E in south korea: Challenges and opportunities," *IEEE Communications Magazine*, vol. 62, no. 1, pp. 112–118, 2024.

[22] P.-Y. Ho, L. Lee, Y.-T. Kuo, C.-C. Chien, Y.-X. Zhan, M.-H. Ho, C.-Y. Huang, Y.-M. Chen, C.-L. Lin, C.-H. Wu *et al.*, "Exploring automated frequency coordination system for 6 GHz wi-fi in taiwan," in *2024 International Computer Symposium (ICS)*. IEEE, 2024, pp. 139–144.

[23] S. Shi, Y. Xiao, W. Lou, C. Wang, X. Li, Y. T. Hou, and J. H. Reed, "Challenges and new directions in securing spectrum access systems," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6498–6518, 2021.

[24] M. Grissa, A. A. Yavuz, and B. Hamdaoui, "TrustSAS: A trustworthy spectrum access system for the 3.5 GHz CBRS band," in *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications*, 2019, pp. 1495–1503.

[25] T. R. Newman, T. C. Clancy, M. McHenry, and J. H. Reed, "Case study: Security analysis of a dynamic spectrum access radio system," in *2010 IEEE Global Telecommunications Conference GLOBECOM 2010*, 2010, pp. 1–6.

[26] A. Bhuyan, X. Zhang, and M. Ji, "Distributed and secure spectrum sharing for 5G and 6G networks," in *2024 IEEE Military Communications Conference (MILCOM)*, 2024, pp. 1–5.

[27] L. Perera, P. Ranaweera, S. Kusaladharma, S. Wang, and M. Liyanage, "A survey on blockchain for dynamic spectrum sharing," *IEEE Open Journal of the Communications Society*, vol. 5, pp. 1753–1802, 2024.

[28] X. Jin, J. Sun, R. Zhang, Y. Zhang, and C. Zhang, "Specguard: Spectrum misuse detection in dynamic spectrum access systems," *IEEE Transactions on Mobile Computing*, vol. 17, no. 12, pp. 2925–2938, 2018.

[29] R. W. West, M. Basit Iqbal Awan, M. Gomez, V. Gopalakrishnan, D. Maas, A. Sivakumar, J. V. der Merwe, and I. Zelaya, "Spectraleas: Dynamic wireless spectrum subleasing," in *2025 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, 2025, pp. 1–10.

[30] R. W. West, D. Maas, D. M. Johnson, and K. Van der Merwe, "Spectracert: A hierarchical system for dynamic spectrum license enforcement," *Proceedings of the ACM on Networking*, Nov. 2025.