DIFFLOC: WiFi Hidden Camera Localization Based on Electromagnetic Diffraction

Xiang Zhang[1], Jie Zhang[2], Huan Yan[3], Jinyang Huang[4], Zehua Ma[1], Bin Liu[1]✉, Meng Li[4], Kejiang Chen[1], Qing Guo[2], Tianwei Zhang[5], Zhi Liu[6]
[1]*University of Sci and Tech of China;* [2]*CFAR and IHPC, A*STAR;* [3]*Guizhou Normal University;* [4]*Hefei University of Tech;* [5]*Nanyang Tech University;* [6]*The University of Elec-Com.*

Abstract

The growing privacy risks posed by hidden WiFi cameras have prompted increasing interest in their detection and localization. However, existing localization solutions suffer from several limitations, such as requiring substantial user effort, large activity spaces, predefined parameters, and pre-collected training data. In this paper, we present DIFFLOC, a novel and low-cost system that localizes hidden WiFi cameras by leveraging the fundamental physical principle of electromagnetic diffraction. When an obstacle passes through the direct path between a transmitter and a receiver, it causes a distinctive signal attenuation pattern. We theoretically analyze the feasibility of using this phenomenon for localization, identifying two critical requirements for building an unbiased diffraction localization model: symmetry and observability. To meet these requirements, DIFFLOC introduces a controllable diffraction generation method. By precisely rotating a small metal plate around a passive WiFi receiver (e.g., a Raspberry Pi), the system produces a consistent and predictable diffraction "shadowing" effect. We then construct an unbiased localization model that maps this effect to the azimuth of the hidden camera. Implemented using commercially available off-the-shelf hardware, DIFFLOC achieves an average angular error of 14.82° across six diverse environments and eleven different camera models, demonstrating its effectiveness. Code, implementation details, and demo are available at: https://github.com/CamLoPA/DiffLoc.

1 Introduction

WiFi-enabled IoT and mobile devices have become ubiquitous across various aspects of daily life, from smart homes to personal devices. By 2030, the number of wireless IoT devices is projected to exceed 29.4 billion [16]. However, the rapid proliferation of these devices has raised significant privacy concerns, particularly due to the increasing prevalence of illegal WiFi-based surveillance. Hidden WiFi cameras have emerged as a preferred tool for malicious actors due to their ease of deployment and remote operation. A survey of 2,023 Airbnb guests found that 58% were concerned about hidden cameras, and 11% reported personally encountering one [3]. This concern is further underscored by projections that the global wireless video surveillance market will grow at a compound annual rate of 16.8% between 2022 and 2030 [9].

Given the significant threat posed by illegal surveillance, several jurisdictions have enacted legislation to address these privacy violations [1]. These legal measures highlight the urgent need for effective methods to detect and locate hidden wireless cameras. While WiFi camera detection methods have become relatively fixed, they often rely on traffic variations induced by user presence or activity in monitored areas [11, 12, 34], current localization techniques still face substantial limitations. Specifically, methods that rely on lens reflections [22, 32, 37] or electromagnetic/thermal emissions [21, 45, 48, 54] are often cumbersome, requiring expensive, specialized equipment, expert knowledge, and exhaustive inspection of every corner of a room. In response to these challenges, recent research has focused on analyzing WiFi traffic or physical layer information, such as Received Signal Strength Indicator (RSSI) and Channel State Information (CSI), to locate wireless cameras. These methods typically require users to move along the perimeter of the room [12, 23, 34] or perform perturbations at various positions and orientations [11, 35] to detect changes in the camera's RSSI or traffic for localization. However, these techniques generally assume nearly empty rooms (free of furniture and other objects) to allow for smooth user movement, a requirement that is impractical in most real-world scenarios. For instance, Lumos [34] requires users to walk several laps along the room's perimeter with an RSSI collection device, while MotionCompass [11] requires users to walk along two orthogonal paths, each crossing both monitored and unmonitored areas. Both methods are challenging to implement realistically in typical indoor environments. To address this limitation, Gu et al. proposed a fingerprinting-based solution, LocCams [7]. LocCams collects CSI fingerprints with the WiFi line-of-sight (LOS) path either blocked or unobstructed by the

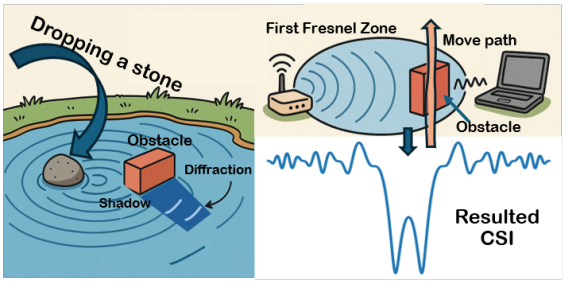


Figure 1: Diffraction-induced attenuation in WiFi.

user's body. It then trains a binary classifier to coarsely infer the quadrant in which the hidden camera is located. While LocCams demonstrates promising performance, it requires pre-collected data for training, making it susceptible to variations in environments and devices. More recently, Zhang et al. introduced CamLoPa [52], which models signal attenuation caused by the user blocking the LOS while walking along two orthogonal paths. This approach eliminates the need for training but depends on several assumed parameters, such as inter-device distances and body dimensions, which introduce non-negligible modeling bias. CamLoPa is also sensitive to inconsistencies in walking speed and irregular user motion, and still requires ample space to accommodate orthogonal walking paths.

Table 1: Qualitative comparison with existing approaches.

Method	Low Cost	No User Efforts	No Training	Space Needed
LAPD [32]	N	N	Y	Low
HeatDeCam [45]	N	Y	N	Low
ESauron [48]	N	N	Y	Medium
Lumos [34]	Y	N	N	High
SNOOPDOG [35]	Y	N	Y	High
MotionCompass [11]	Y	N	Y	High
SCamF [12]	Y	N	Y	High
LocCams [7]	Y	N	N	Low
CamLoPA [52]	Y	N	Y	Medium
DIFFLOC	Y	Y	Y	Low

In this paper, we propose DIFFLOC, a novel approach for hidden WiFi camera localization that addresses the aforementioned limitations. A comparison with existing studies is provided in Table 1. DIFFLOC is inspired by the diffraction mechanism of electromagnetic waves. As illustrated in Figure 1, this concept can be intuitively understood by analogy to water waves. When a stone is dropped into a pond, circular ripples propagate outward. If a brick is placed in the water, it casts a "shadow" behind it, which is an area where the waves cannot pass directly. However, in reality, the waves bend around the brick, and ripples still appear behind it. This bending of waves around an obstacle is known as diffraction. Similarly, when WiFi signals travel between two devices, the majority of the signal energy is concentrated within an elliptical region known as the First Fresnel Zone (FFZ). For WiFi, the FFZ acts like an electromagnetic "pond." When an obstacle enters this zone, it causes significant diffraction [42, 46], resulting in measurable attenuation of the received signal, similar to how water waves fade into smaller ripples after encountering an obstruction. If an obstacle moves through the FFZ, the corresponding signal attenuation pattern can be reflected in the CSI , as shown in the bottom right of Figure 1.

Clearly, a modelable relationship exists between diffraction-induced signal attenuation and the spatial positions of the transmitter and receiver. In essence, attenuation begins when an obstacle enters the FFZ and ends when it exits. In the context of WiFi camera localization, consider a scenario where a monitoring device passively receives signals from a hidden camera while an obstacle moves in a straight, fixed direction near the receiver and intersects the FFZ. If the size of the FFZ is known, the duration of the observed attenuation can reveal the camera's azimuth, as different crossing angles lead to different traversal lengths through the FFZ. However, determining the FFZ's dimensions requires knowledge of the exact distance between the transmitter and receiver, which is typically unavailable in practice. Consequently, similar approaches must assume this distance, inevitably introducing modeling biases. This limitation raises a critical question: **How can we construct an unbiased localization model without knowing the inter-device distance?**

In practice, this can be achieved by ensuring that the obstacle moves along a straight path that crosses the LOS at a 90° angle, as illustrated in Figure 1. In this setup, following the previously described diffraction principle, attenuation begins when the leading edge of the obstacle enters the FFZ and ends when the trailing edge exits. Connecting the two boundary points forms a line segment whose midpoint lies on the LOS. A line drawn from the receiver to this midpoint indicates the direction of the transmitter (camera). Building on this principle, an unbiased localization model must satisfy:
Symmetry. The obstacle crossing the FFZ must move symmetrically with respect to the LOS, meaning that its diffraction path is mirrored on both sides of the LOS. Here, the diffraction path refers to the portion of the obstacle's trajectory that lies within the FFZ. If this symmetry condition is not satisfied, it becomes difficult to infer the direction of the LOS based solely on the obstacle's positions at the start and end of the diffraction period. This raises the following question:

Q1: Since the azimuth of the target camera is unknown, how can we ensure that the obstacle crosses the FFZ in a manner that is symmetric with respect to the LOS?

In addition to symmetry, another key condition must be satisfied to enhance robustness:
Observability. At the start and end of diffraction, attenuation is minimal and prone to being masked by environmental noise, leading to poor observability. In contrast, the region

of maximum attenuation, which includes the trough and its surrounding areas, offers higher observability. However, the peak attenuation period is not the same as the total attenuation duration. Even if the obstacle's movement is symmetric, its relationship with the LOS still depends on the distance between the devices. This introduces the following challenge:

Q2: Without knowledge of the inter-device distance, how can we still leverage the high observability of the maximum attenuation period?

To address these challenges, we propose a novel controllable diffraction generation method. Specifically, DIFFLOC rotates the obstacle around the receiver using the receiver as the center. This rotational motion ensures the following: 1) Symmetry: Regardless of the camera's azimuth, circular motion inherently maintains symmetry with respect to the LOS. 2) Distance Independence: This method ensures that the maximum attenuation period is only minimally influenced by the transmitter–receiver distance. More importantly, this period is symmetrically distributed around the LOS direction. As a result, the localization model can be constructed without relying on distance-related parameters. Further details and supporting evidence are provided in Section 4.2.

Building on the proposed controllable diffraction generation method, we developed an unbiased localization model. The core conclusion of this model is straightforward: the position of the obstacle at the midpoint of the maximum attenuation period lies along the LOS direction. Leveraging this principle, we designed DIFFLOC. The DIFFLOC prototype system utilizes a commercial off-the-shelf (COTS) Raspberry Pi to passively monitor WiFi CSI, while a small metal plate, driven by a stepper motor, rotates around the receiver to generate controllable diffraction. Next, based on the derived localization model, DIFFLOC calculates the orientation of the obstacle at the midpoint of the maximum CSI attenuation period, which directly corresponds to the azimuth of the hidden camera. We evaluated DIFFLOC across six different environments using eleven types of cameras. It achieved an average azimuth localization error of 14.82°, demonstrating robust performance across diverse settings and devices.

In summary, we make the following key contributions:

- We introduce DIFFLOC, a novel and low-cost hidden WiFi camera localization system. DIFFLOC is the first approach to infer camera orientation via controllable diffraction without any parametric assumptions and user effort.
- We systematically identify the symmetry and observability requirements for constructing an unbiased diffraction-based localization model, and propose a controllable diffraction generation method to satisfy both conditions.
- We implement DIFFLOC using low-cost COTS devices and validate its effectiveness through extensive experiments.

2 Background

WiFi CSI captures fine-grained details about how wireless signals propagate between devices [8, 24]. It encompasses a variety of effects, including attenuation, multipath propagation, and phase shifts. This CSI matrix H is commonly expressed as [50]:

$$H(f) = |H(f)|e^{j\theta(f)}, \tag{1}$$

where f is the center frequency, $|H(f)|$ and $\theta(f)$ are the magnitude and the phase shift of the CSI. The CSI magnitude characterizes signal attenuation. The received CSI is a superposition of signals from all propagation paths, and its Channel Frequency Response (CFR) can be represented as [51]:

$$H(f,t) = H_s(f,t) + H_d(f,t) = \sum_{m_s \in \Phi_s} a_{m_s}(f,t)e^{-j2\pi\frac{d_{m_s}(t)}{\lambda}} + \sum_{m_d \in \Phi_d} a_{m_d}(f,t)e^{-j2\pi\frac{d_{m_d}(t)}{\lambda}}, \tag{2}$$

where $H_s(f,t)$ and $H_d(f,t)$ represent the static and dynamic components, respectively. Φ_s denotes the set of static paths, such as those reflected off walls, furniture, and static body parts, while Φ_d represents the set of dynamic paths, such as those reflected off moving objects or people. Therefore, when an object moves within the sensing area, the CSI can be used to characterize the signal attenuation caused by its movement. t, $a_m(f,t)$, $d_m(t)$, and λ represent the timestamp, complex attenuation, propagation distance, and the signal wavelength, respectively. CSI was introduced in the IEEE 802.11n standard in 2009, and devices supporting earlier standards now account for only a small fraction of the market [14]. Tools like csitool [10], picosense [20], and nexmon_csi [6, 33] can be used to extract CSI from various network cards, such as the Intel 5300, AX210/AX200, and bcm43455c0 (Raspberry Pi B3+/B4).

3 Overview

3.1 Threat Model

We focus on scenarios such as short-term rentals (e.g., Airbnb), hotel rooms, and offices where users expect privacy but attackers can temporarily gain physical access. For example, a malicious host may install a WiFi-enabled spy camera in a rental apartment before the guest arrives, or an employee may covertly place a camera in an office [27, 34, 40]. These scenarios are further supported by several real-world cases [4, 15], where attackers have been caught live-streaming users in private spaces, and live-streaming offers a more practical and scalable solution from a management perspective [35]. The user's goal is to detect and localize the hidden camera. In this paper, we focus on WiFi as the communication channel,

consistent with recent works [7,12,34,35], as WiFi is the most commonly used method for remote surveillance with commercially available consumer devices. Below, we describe the real-world settings for both the attacker and the user.

Attacker: The attacker has deployed a WiFi camera within a specific area for surveillance purposes.

- The attacker has full control over the environment for a limited duration, allowing them to modify the space and install a WiFi-enabled hidden camera. To effectively monitor private activities, the camera is typically positioned to avoid obstructions and to maximize its field of view [28].
- The attacker has complete control over the deployed camera and the connected WiFi network via an app or web interface. This includes the ability to control the camera for monitoring victims, configure the WiFi's channels, encryption methods, and access modes.
- The deployed camera is a COTS device. Similar to current studies [29,34,36,52], we assume the attacker does not alter the camera's firmware, network protocols, or wireless transmission behaviors, as such modifications typically require advanced technical expertise.

User: The user aims to detect and localize the hidden WiFi camera deployed by the attacker.

- For portability, the user typically carries only a small device and has no prior knowledge of the target camera or any exploitable vulnerabilities.
- The user has control over the target space, including all WiFi devices within the space. However, their movement may be constrained by furniture or layout, making it difficult to implement existing solutions that require extensive walking or space [11,12,34,35,49].
- The user does not have control over the WiFi network to which the camera is connected and cannot collaborate with the camera. However, they can passively sniff 802.11 packets transmitted by the camera and extract CSI.

3.2 Workflow of DIFFLOC

Given that WiFi camera detection technologies have become relatively fixed, this paper focuses on the more challenging task of WiFi camera localization, a field that still faces several limitations. In this subsection and in Section 4, we present DIFFLOC specifically from the localization perspective. A comprehensive description of the hidden camera detection and localization system we developed is provided in Section 5. The workflow of DIFFLOC, as illustrated in Figure 2, consists of two distinct phases:

Data Collection. DIFFLOC requires the user to provide the MAC address of the target device and the 802.11 channel on which it operates. This information can be easily acquired using sniffing tools and a network card in monitor mode. Once obtained, DIFFLOC passively monitors the target device's traffic, continuously extracting CSI without alerting the target device. While recording CSI, DIFFLOC controls a stepper motor to move an attached metal plate along a predefined path, thereby introducing controllable diffraction attenuation. This attenuation is then captured in the CSI amplitude.

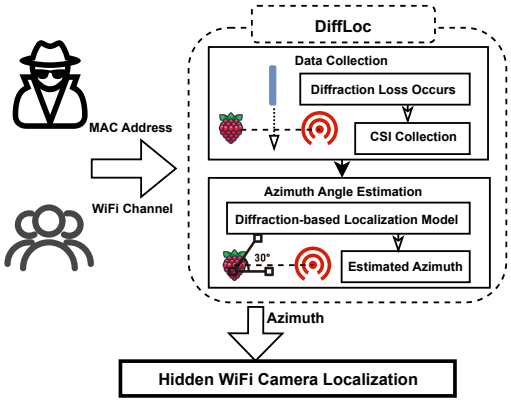


Figure 2: Workflow of DIFFLOC.

Azimuth Angle Estimation. DIFFLOC preconstructs a model that defines the relationship between variations in controlled diffraction attenuation and the angle between the metal plate and the target device. During operation, DIFFLOC tracks the angular trajectory of the plate's movement. It then uses the signal attenuation, captured in the CSI, to fit the preconstructed model and identify the moment when the theoretical angle between the plate and the target device reaches zero. At this point, the angle of the metal plate's movement corresponds to the azimuth angle of the target device.

4 Localization Based on Diffraction

In this section, we present the principle of using electromagnetic diffraction for WiFi camera localization. We begin by explaining the concept of the Fresnel zone, which provides an intuitive understanding of the diffraction and attenuation effects on electromagnetic wave signals. The Fresnel zone can be visualized as a series of concentric ellipses as shown in Appendix A, with the transmitting and receiving devices serving as the foci of these ellipses. The equation describing the ellipse is given by [31]:

$$|TxQ_n| + |Q_nRx| - |TxRx| = n\lambda/2, \tag{3}$$

where Q_n represents a point on the boundary of the n-th Fresnel zone, with Tx and Rx denoting the electromagnetic wave transmitter and receiver, respectively. The phase difference of waves within the FFZ is relatively small, and a significant portion of the signal energy is concentrated in this region.

In wireless communication and wave propagation, energy within the FFZ typically accounts for approximately 60%-70% of the total transmitted energy. Obstacles outside the FFZ primarily affect the signal through reflections. As the energy outside the FFZ is relatively low, obstacles beyond this zone have minimal impact on overall communication energy, causing only slight signal attenuation [44, 46, 47]. In contrast, obstacles within the FFZ primarily cause diffraction [5, 31]. Since a substantial portion of the signal energy is transmitted within the FFZ, any diffraction-induced attenuation leads to significant signal energy loss, which is clearly reflected in the CSI magnitude. In summary, **obstacles passing through the FFZ cause diffraction of electromagnetic wave signals, resulting in significant energy attenuation.**

4.1 Diffraction Attenuation in WiFi

During WiFi signal propagation, diffraction allows radio waves to bend around the Earth's curvature, extend beyond the horizon, and travel behind obstacles [31]. According to Huygens' principle, each point on a wavefront acts as a source of secondary wavelets, which combine in the direction of propagation to form a new wavefront. Diffraction occurs when these secondary wavelets spread into regions that would otherwise be shadowed. Below, we provide a detailed description of diffraction and its resulting attenuation in a system consisting of a pair of WiFi transceivers.

Figure 3 illustrates a schematic of the FFZ created by a pair of WiFi transceivers. Suppose a metal plate moves through the FFZ. The height of a point Q from the line-of-sight (LOS) path is h, and its projections onto the LOS path have distances d_1 and d_2 from Tx and Rx, respectively. The phase difference Δd between the signal passing through this point and the LOS path can be expressed as [31]:

$$\phi = \frac{2\pi\Delta d}{\lambda} = \frac{\pi h^2}{\lambda}\frac{d_1+d_2}{d_1 d_2} = \frac{\pi}{2}v^2. \tag{4}$$

Here, Δd is the path difference, and v is the Fresnel-Kirchoff diffraction parameter:

$$v = h\sqrt{\frac{2(d_1+d_2)}{\lambda d_1 d_2}}. \tag{5}$$

The variable v combines the Fresnel approximation with Kirchhoff's diffraction theory and is used to describe the diffraction effects when a wave encounters an obstacle or aperture. The value of v determines the degree of diffraction: smaller values of v correspond to less significant diffraction, typically caused by a tiny obstacle or greater distance, while larger values indicate more pronounced diffraction as the wave bends around an obstacle.

The radius of the FFZ (i.e., the perpendicular distance from

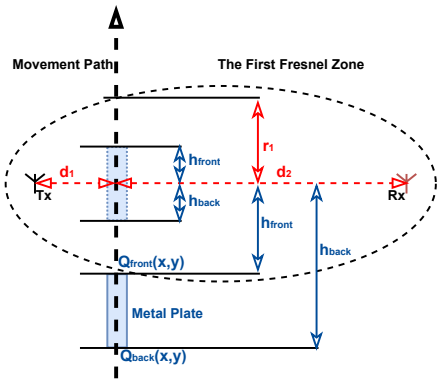


Figure 3: A moving metal plate across the FFZ.

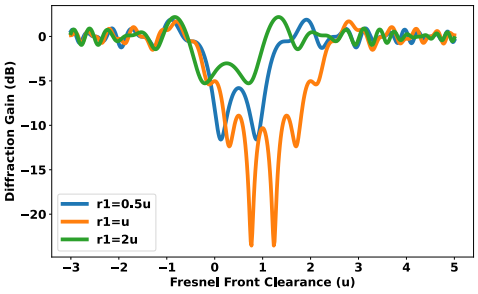


Figure 4: Diffraction gain corresponding to Figure 3.

point Q to the LOS path) can be calculated as [31]:

$$r_1 = \sqrt{\frac{\lambda d_1 d_2}{d_1+d_2}}. \tag{6}$$

Thus, the diffraction parameter v can also be expressed as:

$$v = h\sqrt{\frac{2(d_1+d_2)}{\lambda d_1 d_2}} = h\frac{\sqrt{2}}{r_1}. \tag{7}$$

In wireless communication systems, only a portion of a signal's energy diffracts around an obstacle, allowing some of the blocked energy to reach the receiver. When an obstacle partially obstructs the Fresnel zone, the received energy is the vector sum of the contributions from all unobstructed sections of the Fresnel zone [31]. For an infinitely long object positioned at a height h from the LOS path, the ratio of the diffracted electric field strength E_d to the unobstructed electric field strength E_o is given by:

$$\frac{E_d}{E_o} = F(v) = \frac{1+j}{2}\int_v^\infty \exp\left(\frac{-j\pi t^2}{2}\right)dt, \tag{8}$$

where $F(v)$ represents the complex Fresnel integral.

For a finitely size obstacle, as in Figure 3, both ends of the plate create diffraction effects, with h_{front} and h_{back} representing the heights from the front and back edges of the plate to

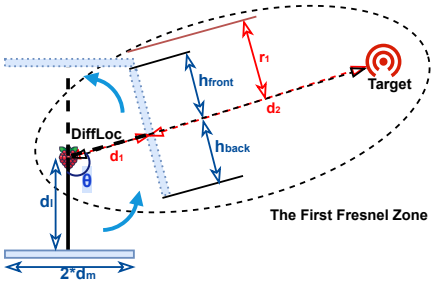


Figure 5: Controllable diffraction design in DIFFLOC.

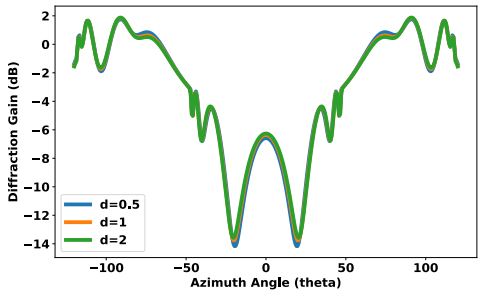


Figure 6: Diffraction gain corresponding to Figure 5.

the LOS path, respectively. The attenuation due to diffraction at these edges can be expressed as:

$$F(v_{front}) = \frac{1+j}{2}\int_{v_{front}}^{\infty} exp(\frac{-j\pi t^2}{2})dt, \quad (9)$$

$$F(v_{back}) = \frac{1+j}{2}\int_{-\infty}^{v_{back}} exp(\frac{-j\pi t^2}{2})dt. \quad (10)$$

The diffraction gain due to the presence of the finitely size plate is given by:

$$G_d(dB) = 20log|F(v_{front}) + F(v_{back})|. \quad (11)$$

4.2 Principle of Diffraction Based Localization

Using equations 9, 10, and 11, we illustrate the diffraction attenuation caused by a metal plate with width $2d_m$ passing through the FFZ, as shown in Figure 4. u represents the Fresnel clearance [47], which indicates the percentage of the plate that crosses the LOS path. It is defined as:

$$u = \frac{h}{r_1}, \quad (12)$$

In Figure 4, u represents u_{front}, and it is evident that attenuation occurs when the obstacle is in the FFZ. This inspires the design of DIFFLOC. Specifically, if an obstacle crosses the FFZ perpendicular to the LOS, as shown in Figure 3, the obstacle induces diffraction from the moment it enters until it fully exits the FFZ as shown in Figure 4. If the position of the obstacle is known at each moment, the line connecting the receiver's location to the midpoint between the point Q_{front} at the start of attenuation and Q_{back} at the end of attenuation, indicates the LOS direction. This line also points towards the transmitter. Therefore, if the receiver's location is known and the positions of the obstacle during diffraction are tracked, azimuth localization can be achieved. In real-world scenarios, to ensure that the diffraction behavior can be reliably modeled, the obstacle's motion should be kept as simple and controlled as possible. Additionally, to develop an unbiased localization model based on this principle, two conditions must be satisfied:

- **Symmetry of diffraction:** The obstacle's movement must be symmetric with respect to the LOS. If this symmetry is not satisfied, e.g., if the obstacle crosses the FFZ at an angle other than 90 degrees, it becomes difficult to relate the observed diffraction attenuation pattern to the LOS direction, as this introduces an additional unknown variable: the crossing angle.

- **Observability:** As illustrated in Figure 4, the attenuation at the start and end of diffraction is relatively small and can easily be overshadowed by environmental and hardware noise in practical settings. In contrast, the period of maximum attenuation (i.e., the trough) is more robust and reliably observable. However, accurately calculating the positions of the troughs requires knowing the Fresnel clearance u, which in turn depends on the distance d between the transmitter and the receiver. In practical scenarios, obtaining d is challenging.

DIFFLOC addresses these two conditions by designing a novel controllable diffraction attenuation. Specifically, DIFFLOC makes a metal plate rotate around the receiver to create diffraction, as shown in Figure 5. This method ensures that the plate's path is symmetric relative to the LOS, regardless of the position of the transmitting device. The dimensions of the metal plate ($2*d_m$) and its distance from the receiver (d_l) are controllable. The only unknown factor is the distance between DIFFLOC and the target device (d). Given the angle between the plate and the LOS (θ), the positions of the metal plate at each moment, represented by u_{front} and u_{back}, can be be calculated as:

$$u_{\text{front}} = d_l \cdot \sin(\theta) + d_m \cdot \cos(\theta), \quad (13)$$

$$u_{\text{back}} = d_l \cdot \sin(\theta) - d_m \cdot \cos(\theta), \quad (14)$$

The distances from the receiver to the projections of the front and back edges onto the LOS path are:

$$d_{\text{front}} = d_l \cdot \cos(\theta) - d_m \cdot \sin(\theta), \quad (15)$$

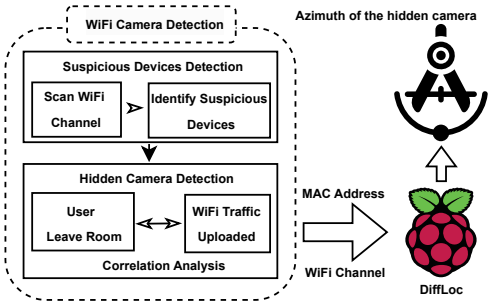


Figure 7: Framework of the DIFFLOC-based hidden WiFi camera detection and localization system.

$$d_{\text{back}} = d_l \cdot \cos(\theta) + d_m \cdot \sin(\theta). \tag{16}$$

Then the diffraction parameter can be calculated as:

$$v_{front} = \sqrt{2}u_{front} / \sqrt{\frac{\lambda \cdot d_{\text{front}} \cdot (d - d_{\text{front}})}{d}}, \tag{17}$$

$$v_{back} = \sqrt{2}u_{back} / \sqrt{\frac{\lambda \cdot d_{\text{back}} \cdot (d - d_{\text{back}})}{d}}. \tag{18}$$

Finally, the relationship between diffraction gain and θ, calculated using 9, 10 and equation 11, is illustrated in Figure 6. It is evident that the position of the troughs is nearly independent of d, and most importantly, the period of maximum diffraction attenuation is centered around $\theta = 0$. In summary, the period of maximum CSI attenuation corresponds to the time when the metal plate faces the target device. By analyzing the recorded CSI, which characterizes the attenuation, DIFFLOC matches the recorded rotation angle of the plate with the attenuation loss variation captured in the CSI, thus achieving localization. Specifically, DIFFLOC records the rotation angle of the metal plate at each moment as it spins. Once CSI collection is complete, the system identifies the time period during which the maximum CSI attenuation (the troughs) occurs. The rotation angle of the metal plate at the midpoint of this time period corresponds to the azimuth angle of the target device, θ_d.

5 WiFi Camera Detection and Localization

In this section, we introduce the hidden WiFi camera detection and localization system based on DIFFLOC, as shown in Figure 7. The system is composed of two key components: WiFi camera detection and DIFFLOC-based localization. The detection component identifies potential hidden cameras by analyzing the correlation between WiFi traffic and user activity, similar to previous studies [7, 34, 52]. It then provides the camera's MAC address and corresponding WiFi channel to DIFFLOC, which determines the camera's azimuth. In the hidden camera localization scenario, since the hidden camera must remain unobstructed to monitor the target area, its location can be easily determined by identifying the first obstacle along the detected azimuth angle. Below, we describe the detailed process of the WiFi hidden camera detection and localization.

Following the approach proposed in prior work [7, 34, 52], WiFi camera detection consists of two stages: suspicious device detection and hidden camera detection. The goal of suspicious device detection is to narrow the scope of analysis. Given the large number of WiFi devices in everyday environments, analyzing all devices would be inefficient. Therefore, an initial filtering step is required to identify suspicious devices. Video streams typically involve large data volumes, characterized by relatively large and stable upload traffic. Hence, the system first scans the surrounding WiFi networks to detect all access points (APs), including those with hidden SSIDs. According to [26], DIFFLOC excludes APs that fail to meet the minimum RSSI requirement for video streaming, which is below -67 dBm (with a 5dBm buffer applied to avoid misdetection). The system then sequentially scans the channels of the remaining APs, sniffing and capturing 802.11 packets to determine if any devices are continuously uploading data. For the captured WiFi packets, the system clusters them by source MAC address, filters out Management-Type and Control-Type frames, and retains only Data-Type frames for further analysis, as application layer data is encapsulated within these frames [18]. The system then calculates the average payload size of Data-Type frames for each device and filters suspicious devices based on the following criteria:

$$\mathbf{S_{mac}} = \begin{cases} \textbf{true} & \text{if } \bar{s}_{mac} > T_s \& l > T_l \& \textbf{mac} \neq \textbf{m}_{\textbf{ap}}, \\ \textbf{false} & \text{else .} \end{cases} \tag{19}$$

Here, $\mathbf{S_{mac}}$ represents the determination of whether the device with MAC address **mac** is suspicious. $\bar{s}_{mac}$, T_s, l, $\mathbf{m_{ap}}$, and T_l denote the average size of all packet payloads, the size threshold, the count of packets, the MAC address of APs, and the count threshold, respectively.

The system then sends the MAC address and corresponding 802.11 channel of each suspicious device to the hidden camera detection module for further evaluation. The core principle of this module is that, before uploading video streams, cameras typically compress data through encoding to reduce the upload volume. Video compression standards, such as H.264 [38] and H.265 [30], achieve high compression rates through inter-frame prediction. These standards use different frame types—Intra-coded (I), Predicted (P), and Bi-directionally Predicted (B) frames—to compress video. When there is activity in the monitored area, the number of P and B frames increases, leading to a higher upload traffic rate [12, 35]. In contrast, in static scenarios, the traffic rate decreases. Our system leverages this causal relationship between activity and traffic to detect hidden cameras. Specifically, the system prompts the user to leave the room and then calculates the data throughput of each suspicious device per

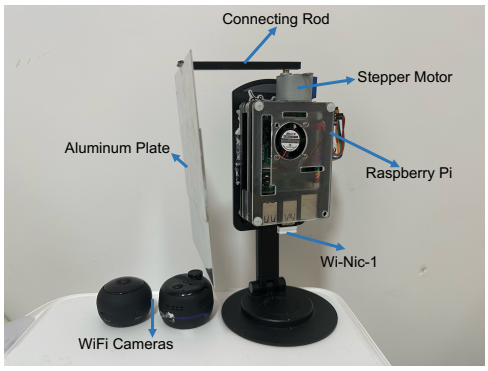


Figure 8: The prototype of DIFFLOC.

second, looking for patterns where throughput is initially high and subsequently decreases after the user leaves. If such a pattern is detected, the device is flagged as a potential hidden camera. More details about hidden WiFi camera detection please refer to Appendix C. Once a hidden WiFi camera is identified, the system passes the camera's MAC address and corresponding WiFi channel to the DIFFLOC module for localization. The user then uses the θ_d provided by DIFFLOC to search for the hidden camera. In typical indoor surveillance scenarios, a hidden camera must have a clear LOS and cover a sufficiently large area to effectively monitor a target. Therefore, it is highly likely that the camera is concealed within the first object encountered along the indicated direction [52].

6 Implementation and Evaluation

6.1 Prototype

The DIFFLOC prototype is shown in Figure 8. The Raspberry Pi uses its built-in wireless network interface card (NIC), modified with the Nexmon csi tool [6], to extract CSI. Since the NIC operates in monitor mode during CSI extraction, it cannot handle communication. Therefore, an external USB WiFi adapter (Wi-Nic-1) is used for communication. To create diffraction, we use a plug-and-play peripheral consisting of a stepper motor, control board, stand, 3D-printed connecting rod, and a thin aluminum plate. The aluminum plate is 10 cm wide, which is sufficient to induce significant diffraction, as obstacles with dimensions comparable to or larger than the signal wavelength (approximately 12 cm for 2.4 GHz and 6 cm for 5 GHz) cause notable diffraction effects. The connecting rod is 8 cm long; although this length may slightly influence the angular position of attenuation troughs relative to the LOS, the troughs remain centered around the LOS, thereby preserving the validity of the unbiased localization model. Since the modified driver does not support packet sniffing, we set up an additional external network card (Wi-Nic-2) with monitoring capabilities to capture 802.11 packets. More details of the implementation can be found in Appendix D.

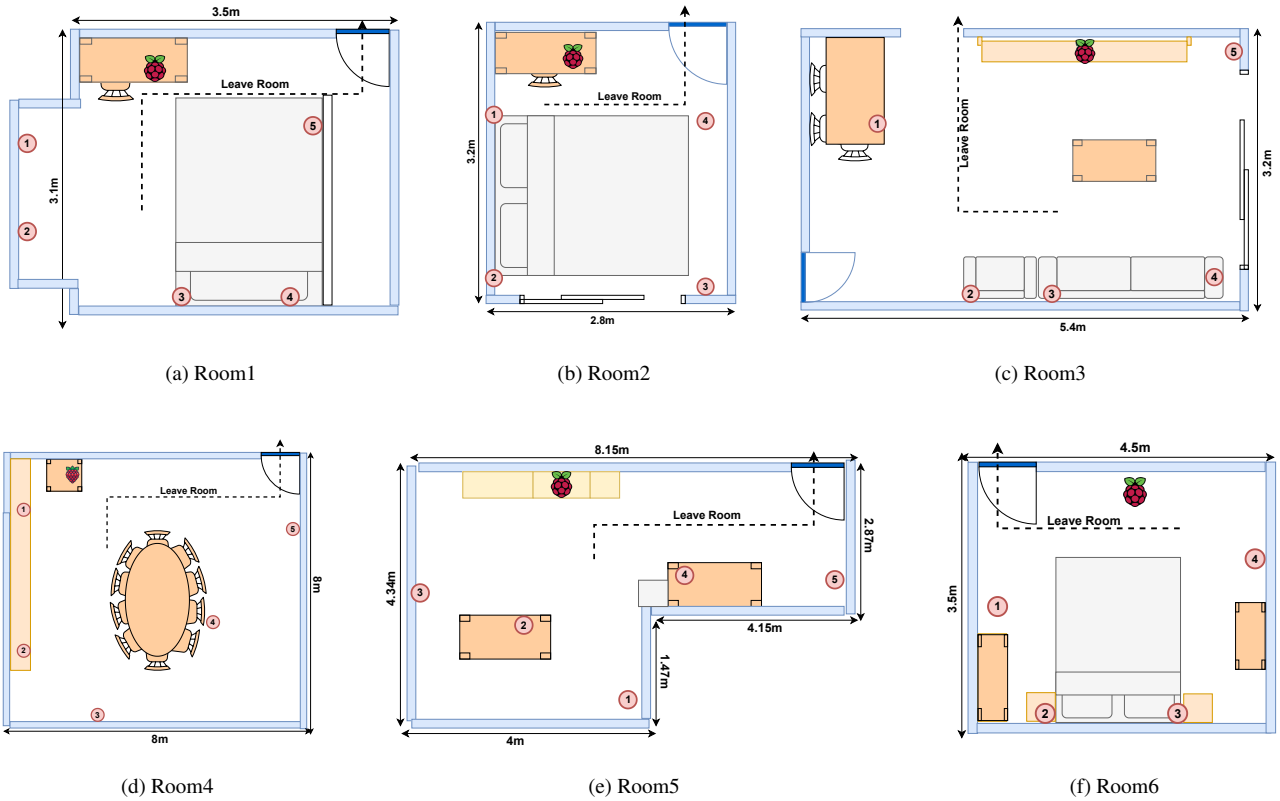
6.2 Experimental Setup

Our experiments evaluate hidden WiFi camera localization across six distinct environments using eleven different camera models. The devices used in the experiments are listed in Table 2, with all devices purchased from online platforms. Cameras were selected by searching popular e-commerce websites with relevant keywords (e.g., "WiFi camera," "mini camera") and choosing models based on sales volume and popularity. For the localization task, the system is typically placed near a wall (e.g., on a table or windowsill) to facilitate deployment. DIFFLOC is configured to collect CSI data only while the metal plate moves within the 0-180 degree range, due to signal interference caused by metal components on the back side of the Raspberry Pi's printed circuit board (PCB). The stepper motor completes 512 steps per full revolution, with each step consisting of 8 microsteps and a delay of 0.0015 seconds between microsteps. As a result, the motor takes approximately 3.07 seconds to rotate 180 degrees. To account for buffer time, the CSI collection period for each localization process is set to 5 seconds. In our experiments, T_s and T_l are set to 300 bytes and 150 packets, respectively, based on the observed transmission rates of 5 kinds of real cameras (Table 3). Since the Nexmon tool allows extraction of CSI from a specified MAC address in monitor mode, there is no need for AP coordination or substitution during the process.

Table 2: Devices used in experiments.

Device	Abbreviation
XiaoMi Cloud Camera2	Mi
360 Cloud Camera 6C	360
HiLEME Mini Camera2	Hi2
360 Cloud Camera 8Pro	8P
Mingshen Mini Camera	Ms
Guangchun Mini Camera	Gc
EZVIZ C2C	C2C
HiLEME Mini Camera	Hi
XiaoMi Cloud Camera3	Mi3
Guangchun Mini Camera2	Gc2
BangshiDa Mini Camera	Bs

Our experiments were conducted in six realistic rooms across four distinct environments, with the layouts shown in Figure 9. Rooms 1–3 are located within the same residential apartment, a real-world home environment filled with typical obstacles such as furniture and household items. Specifically, Rooms 1 and 2 (Figures 9a and 9b) are bedrooms, while Room 3 (Figure 9c) is a living room. These rooms differ in clutter levels: Room 2 is the most cluttered, while Room 3 is the most spacious. Rooms 4–6 are each situated in separate environments. Room 4 (Figure 9d) is a meeting room on a university campus, and Room 5 (Figure 9e) is a university office. Both are significantly larger than the residential spaces, with maximum widths exceeding 8 meters, and the longest



(a) Room1 (b) Room2 (c) Room3

(d) Room4 (e) Room5 (f) Room6

Figure 9: The layout of six rooms and cameras deployment.

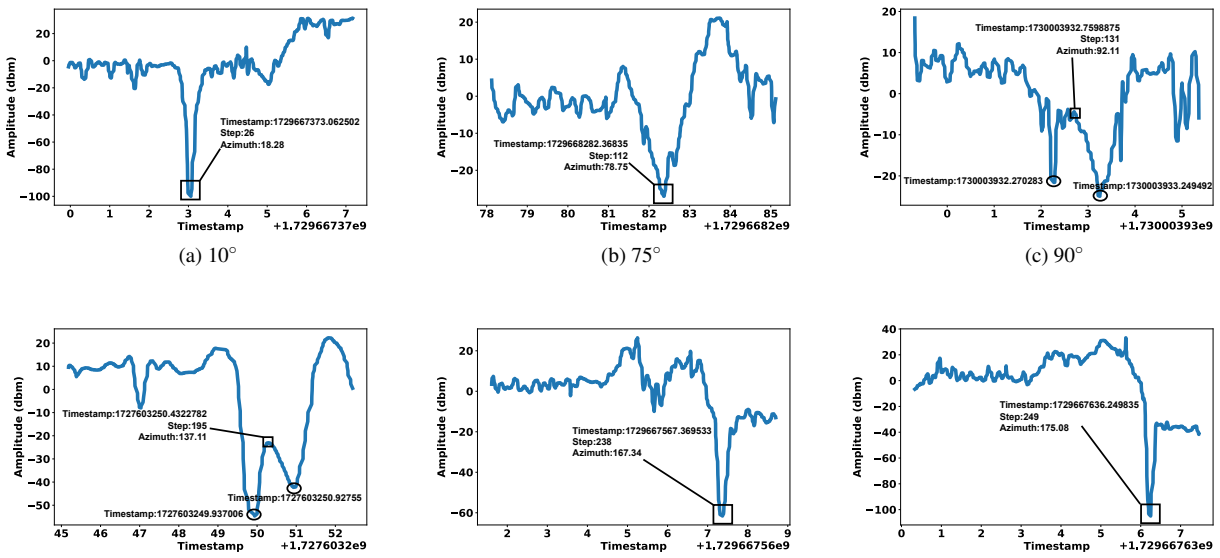
distance between the camera and the localization device reaching approximately 8 meters. Room 6 (Figure 9f) is a bedroom in another residential apartment and is slightly larger than Rooms 1 and 2. Notably, wall materials vary across rooms; for example, Rooms 2 and 3 feature a sliding door made of metal and glass that occupies nearly an entire wall. The experiments were conducted collaboratively by two groups of authors in their respective apartments and offices across different geographic regions. The cameras tested in Rooms 1–3 were the first eight models listed in Table 2, while those used in Rooms 4–6 correspond to the last five models. To enable effective hidden camera search, the user first exited the room to trigger the traffic variations required for detection. Localization was then automatically performed by DIFFLOC using the MAC address and channel index of the detected camera. During this process, the camera was placed at various locations in accordance with the attacker's intent as described in the threat model. As shown in Figure 9, the azimuth angles (relative to the DIFFLOC device's position) for Room 1 were 30.47°, 45.47°, 101.07°, 131.01°, and 163.30°; for Room 2 were 35.22°, 69.30°, 123.69°, and 156.57°; for Room 3 were 20.24°, 59.62°, 80.91°, 119.98°, and 180.00°; for Room 4 were 65.54°, 76.87°, 105.11°, 130.53°, and 162.18°; for Room 5 were 36.26°, 77.11°, 104.78°, 138.38°, and 157.77°; and for Room 6 were 51.67°, 76.70°, 105.74°, and 150.95°.

Table 3: Packet length and rates of each camera.

Device	Mi	C2C	360	Gc	Hi
Packet Length	1050	632	873	640	828
Packet/s	51	63	57	112	130

6.3 Algorithm Implementation and Examples

In this section, we present the algorithmic implementation of DIFFLOC, accompanied by several examples that illustrate the relationship between diffraction-induced attenuation and the target's azimuth. These examples demonstrate the effectiveness of DIFFLOC in real-world scenarios. The core task of DIFFLOC in localizing the WiFi camera is identifying the midpoint of significant attenuation caused by diffraction. Several examples are provided in Figure 10. Due to factors such as distance, movement speed, and multipath effects, the attenuation observed in the CSI can appear in two forms: one that aligns with simulated results, featuring two distinct troughs (e.g., Figures 10c and 10d), and another with only a single trough (e.g., Figures 10a and 10f).



(a) 10° (b) 75° (c) 90°

(d) 135° (e) 170° (f) 180°

Figure 10: Six examples of DIFFLOC. The title indicates the device's orientation. The figures display the identified midpoint of diffraction attenuation, the current stepper motor position, and the corresponding prediction of DIFFLOC, respectively.

DIFFLOC first applies a low-pass filter to the CSI waveform to remove noise. Next, it selects the five subcarriers with the highest mean values for fusion, as these tend to be less susceptible to interference. The system then identifies all the troughs in the CSI. These troughs correspond to significant diffraction-induced attenuation. DIFFLOC searches for a second trough near the lowest one, with a similar amplitude. If such a second trough is found, the midpoint between the two troughs is selected as the localization timestamp. If no second trough is identified, the timestamp corresponding to the lowest trough is used. Once the localization timestamp is determined, DIFFLOC retrieves the recorded timestamps for each step of the stepper motor's movement and identifies the closest match. The angle of the stepper motor at that step is then taken as the azimuth angle. Figure 10 shows the localization results of DIFFLOC when a camera is placed at different locations. DIFFLOC successfully identifies the midpoint of significant attenuation, providing accurate azimuth predictions even in challenging conditions with substantial interference (e.g., Figure 10c). More details please refer to our released code.

6.4 Evaluation of WiFi Camera Localization

Detection and false positive: We conducted a total of 140 hidden camera detection experiments across Rooms 1–3. Our hidden WiFi camera detection and localization system achieved detection success rate of 97.86%. To evaluate the false positive rate, we set up a computer uploading files and another computer and smartphone engaged in video conferencing in Room 1, simulating typical traffic patterns that might be confused with camera traffic. The results showed that only 6.67% of samples resulted in false positives. A detection is considered successful if the system correctly identifies the MAC address of the hidden camera. A false positive occurs when the system mistakenly identifies another device as a hidden camera. Notably, most indoor devices that generate significant traffic are typically under user control, making them less likely to interfere with the detection system. Devices in neighboring rooms, even if they do cause false alarms, would only increase the workload without posing a real security risk.

Localization and error analysis: We conducted five localization trials for each camera model at every deployment position in each room. The localization results across six different rooms are shown in Figure 11, and the localization results for each trial in every room are presented as box plots in Figure 12. DIFFLOC achieved an average azimuth localization error of 14.82 degrees. As shown in Figure 11 and 12, the largest localization errors tend to occur at smaller azimuth angles. For other positions with relatively high errors, such as the 160° deployments in Room 1 and Room 4, we found that in some cases, there were abnormally sharp attenuation troughs near 0° (e.g., at 162.18° in Room 4, the system occasionally produced incorrect azimuth estimates near 0°). In these cases, although a secondary trough often appeared near the correct azimuth, it was less prominent than the spurious dip. As a result, the algorithm sometimes mistakenly selected the spurious dip or a midpoint between the spurious and true troughs, leading to moderate angular deviation in the local-

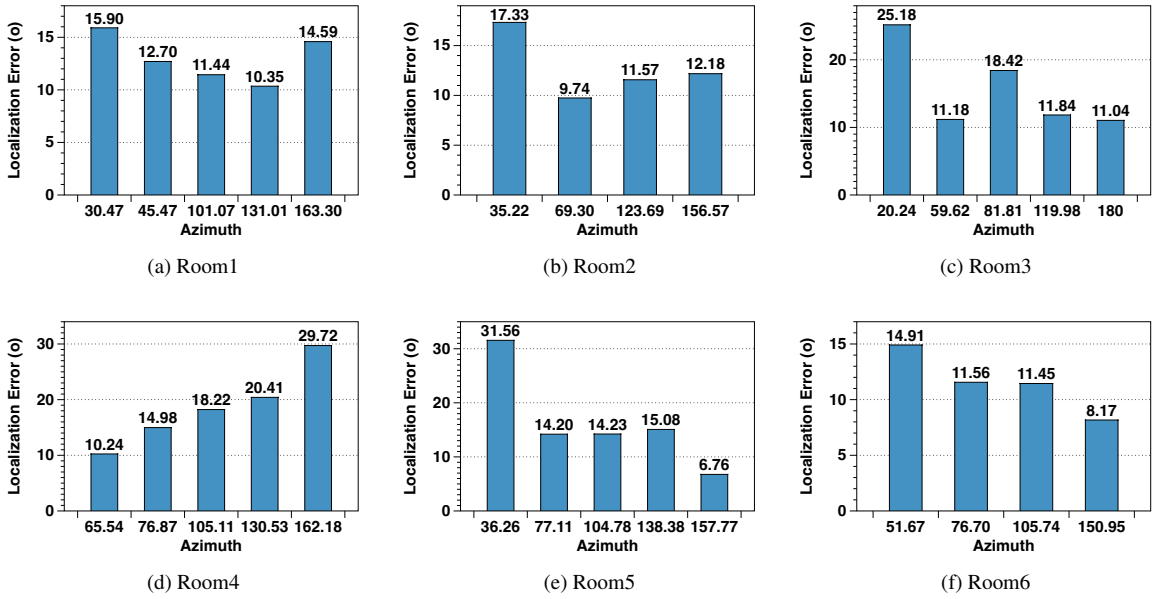


Figure 11: Localization errors of hidden cameras deployed at different rooms. The x-axis represents the azimuth of the camera deployment, while the y-axis shows the average localization error at each position.

ization result. We believe that this bias is introduced by the hardware configuration of the Raspberry Pi. Specifically, its onboard antenna is positioned on the right side of the PCB (near 180°), while the left side (near 0°) contains various components and metallic structures that may obstruct signal propagation and cause interference. This insight highlights a potential avenue for future optimization, which we discussed in Section 7.

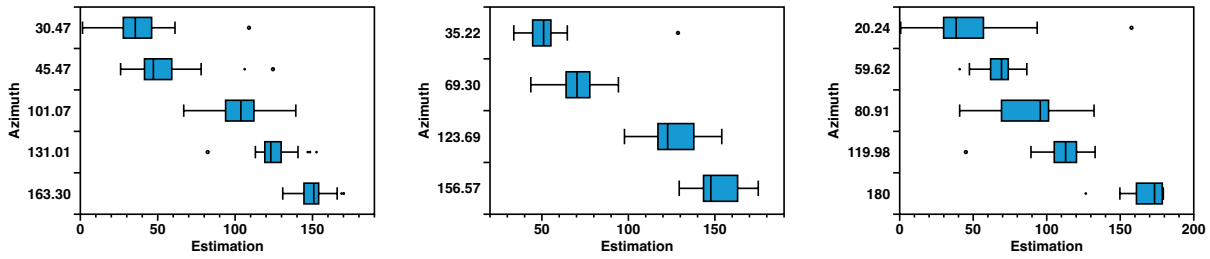
Robustness: Figure 13 illustrates the system's localization performance across a variety of camera models. As shown, the DIFFLOC-based localization system maintains consistent performance across different cameras, demonstrating its robustness to device variations. The average localization errors across Rooms 1–6 were 13°, 12.7°, 15.53°, 18.71°, 16.37°, and 11.53°, respectively, further demonstrating the system's robustness across diverse environmental conditions. Slightly higher errors were observed in larger rooms, particularly in Room 4 where the maximum distance between the camera and the receiver was approximately 8 meters. The increased distance results in weaker WiFi signals and greater susceptibility to noise. In comparison to existing methods, our approach does not require training, user efforts, or assumed parameters. It relies entirely on the theoretical model, ensuring robustness to environmental and device variations.

6.5 NLOS Placement Analysis

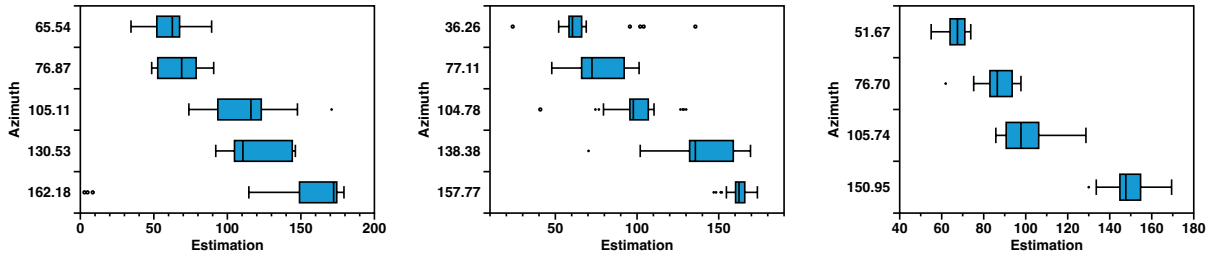
In this section, we analyze scenarios in which the hidden camera is not within the LOS of DIFFLOC, including cases where the camera is concealed by objects and positioned above or below the DIFFLOC device.

In real-world settings, attackers may use various objects to disguise hidden cameras. To assess the performance of DIFFLOC under these conditions, we evaluated its effectiveness when cameras were concealed by different materials. We selected three commonly encountered materials: plastic, fabric, and metal. Many household items that are suitable for hiding cameras, such as power outlets and decorative ornaments, are typically made from these materials. Specifically, the plastic concealment scenario involved placing the camera inside a plastic box; the textile test involved embedding the camera in a stuffed toy; and for the metal condition, the plastic box was internally lined with aluminum plates. To optimize evaluation time, only three camera models were selected. These models were chosen to represent both high and low localization accuracy, ensuring coverage of a diverse performance spectrum. The results, shown in Table 4, indicate that materials like plastic and textiles had little impact on the system's performance. In contrast, metal significantly degraded performance. This is because metal absorbs wireless signals, which not only affects DIFFLOC's ability to locate the camera but also degrades overall network communication quality. Consequently, attackers are unlikely to use metal to conceal cameras.

We further evaluated additional NLOS scenarios in which the camera was placed near the ceiling or floor. When the camera is positioned directly above or directly below the DIFFLOC device, the rotating metal plate cannot intersect the FFZ, resulting in the absence of observable diffraction attenuation and thus preventing localization. However, in real-world deployments, it is relatively rare for a camera to be placed ex-



(a) Room1 (b) Room2 (c) Room3



(d) Room4 (e) Room5 (f) Room6

Figure 12: Box plot of hidden camera localization results across different rooms. The x-axis represents the azimuth estimated by DIFFLOC, and the y-axis shows the ground-truth. Box plot illustrates the distribution of localization results of each trail.

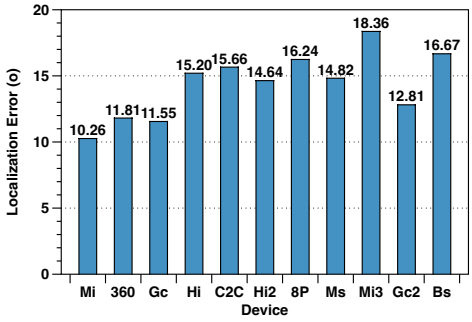


Figure 13: Localization errors across different devices. The x-axis represents the device models, while the y-axis indicates the average localization error of each device.

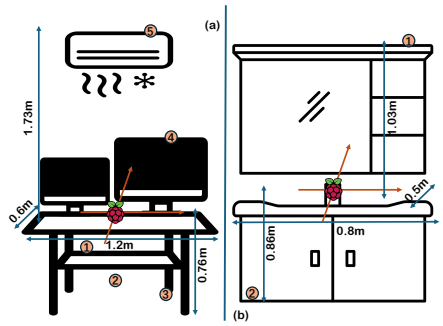


Figure 14: Evaluation Environments for NLOS Scenarios.

actly at these vertical extremes. To further explore the impact of challenging NLOS placements, we conducted experiments in two settings, as illustrated in Figure 14: a desk in Room 1 and a sink in a bathroom. In both cases, the line connecting the camera and the DIFFLOC device was slightly offset from a perfect 90° vertical alignment, meaning the camera was not directly overhead or below, but their horizontal projection distance remained relatively short. We evaluated with the first eight cameras listed in Table 2; the corresponding azimuth angles and localization results are detailed in Table 5 (ordered by environment and index). The results show that localization was still feasible in most cases, even when the horizontal distance was short, due to the inherent width of the FFZ. However, when the horizontal distance becomes very small, the obstacle intersects only a small portion of the FFZ, which may reduce the reliability of localization due to weaker diffraction effects.

6.6 Real-World Search Evaluation

We conducted real-world search experiments to find the hidden camera. Building on the above analysis, our search procedure is described as follows: The user first places DIFFLOC near a wall to initiate detection and localization, recording the detected camera's MAC address and operating channel. The user then searches along the azimuth indicated by the first localization result. If the camera is not located, DIFFLOC is repositioned near the wall in the direction of the previous result, and localization is repeated using the previously recorded

Table 4: Evaluation with Covering (numbers represent localization error in degrees).

Materials	Normal	Plastic	Textile	Metal
360	12.90	12.61	11.19	20.36
Gc	12.19	12.52	13.05	26.67
Hi2	14.65	16.87	12.18	31.46

Table 5: Evaluation Under NLOS Conditions (Po: Placement Azimuth in degrees, Er: Error in degrees).

Po	**143.62**	**90.33**	**31.18**	**59.47**	**72.30**	**56.31**	**148.63**
Er	18.82	29.75	32.65	17.66	16.17	26.53	22.43

MAC address and channel. If the search is still unsuccessful, the device is moved again and the process is repeated. This search procedure helps mitigate errors from challenging angles and NLOS placements. We conducted simulated search experiments using DIFFLOC across the six previously described realistic rooms. Four volunteers participated in the evaluation, with no communication between the individuals responsible for hiding and searching for the hidden camera. Due to the limited number of realistic hiding spots and the natural recall of prior search locations, we did not test every camera in every position. Instead, one volunteer randomly selected a camera and hid it in a location they considered plausible, following the guidance of the threat model, while another volunteer performed the search using the procedure described above. The process was repeated until no additional reasonable hiding spots remained. A search was deemed unsuccessful if the camera was not found after three relocation attempts or within 25 minutes. A total of 27 search trials were conducted. DIFFLOC successfully located the hidden camera in 92.59% of the cases. Among these, 68% of the cameras were found within 9 minutes, 20% within 10–15 minutes, and the remaining 12% within 16–22 minutes.

6.7 Comparative Study

Performance Comparative: Most WiFi based approaches typically evaluate in almost empty rooms and use distance as the evaluation metric [12, 34, 35], which makes comparison with DIFFLOC challenging. Additionally, many of these studies have not been open-sourced. Therefore, we compared DIFFLOC with LocCams [7] and CamLoPa [52], two state-of-the-art systems based on WiFi CSI. LocCams collects CSI while the user holds the device in four different orientations, then uses a pre-trained deep learning model to identify which orientations have their LOS paths blocked. The mid-direction of the blocked LOS paths is then considered the device's azimuth, resulting in a maximum localization resolution of only 45 degrees. CamLoPa estimates the camera's azimuth by analyzing the duration of CSI attenuation as the user walks along two orthogonal paths. However, it relies on assumptions about parameters such as inter-device distance and user body

Table 6: Comparison with Other Methods (numbers represent localization error in degrees).

Method	DIFFLOC	LoID	LoCD	LoCDR	Cam
360	**12.90**	28.30	32.34	46.19	20.97
Gc	**12.19**	26.11	37.88	49.51	19.89

Table 7: Comparison with CamLoPa With Covering (numbers represent localization error in degrees).

Materials	Normal	Plastic	Textile	Metal
CamLoPa	20.12	19.47	19.81	35.15
DIFFLOC	13.25	14.00	12.14	26.16

dimensions, which introduces inevitable modeling biases. It is also sensitive to variations in walking speed and irregular movement. We conducted experiments in Room 2 using two randomly selected cameras (360 and GC) placed at four different locations. The results, shown in Table 6 and 5, include in-domain (ID), cross-device (CD), and cross-device-room (CDR) comparisons for LocCams (Lo), as well as a comparison with CamLoPa (Cam) under conditions where the camera is concealed. The findings clearly demonstrate that DIFFLOC outperforms other methods, exhibiting greater robustness.

Time and User Efforts Comparative: In terms of localization time, LocCams takes approximately 0.5 minutes. CamLoPa takes approximately 1-2 minutes. DIFFLOC only requires 5 seconds, and offering an improvement in robustness. MotionCompass takes around 3 minutes, while other RSSI/traffic-based systems typically require 15-30 minutes [12, 34, 35]. MotionCompass requires the user to walk several straight paths that span both monitored and unmonitored areas, which may be difficult to achieve in real-world environments. Other traffic-based systems require users to walk around the perimeter of each wall or constantly adjust a laptop's position to cover most areas of the room, which is also impractical. For DIFFLOC, the user does not need to move during localization, which makes it more user-friendly.

7 Limitations and Discussions

MAC Address Randomization. While some devices employ MAC randomization [39] to enhance privacy, this does not impact DIFFLOC's localization capabilities. This is because, despite MAC randomization, devices typically use a consistent MAC address once they establish a network connection.

Azimuth Localization, Interference, and Usability. Currently, we focus solely on azimuth localization because users typically do not carry measurement tools to find specific coordinates. Moreover, typical room sizes are relatively small, and cameras are unlikely to be fully obstructed by physical barriers. As a result, identifying the camera's azimuth is a more practical approach to assist users in finding cameras. Since users have control over their environment, they can ensure that

no other individuals are present, thus minimizing potential interference. DIFFLOC features a compact, foldable design, and when collapsed, it is only slightly larger than a Raspberry Pi, ensuring excellent portability (see Appendix E). In future work, we aim to enhance the system's usability by incorporating visual guidance for localization results and developing a more intuitive user interface and software experience.

Evading DIFFLOC. DIFFLOC is designed to locate the WiFi camera deployed by typical attackers. However, more advanced attackers might find ways to evade DIFFLOC. Evading localization would require modifying the network card to manipulate the WiFi signal's CSI, causing it to constantly vary and disrupting the signal attenuation pattern caused by diffraction. This, however, requires specialized knowledge and is technically challenging, as most attackers do not possess the necessary skills. Additionally, modifying network card hardware or firmware is not supported by most commercially available devices. According to recent research [2], most surveillance tools still rely on commercially available devices, thus we have not considered adaptive attacks.

Limitations. DIFFLOC requires a packet rate of 30-50 packets per second for stable performance. If the packet rate is too low or unstable, the diffraction-induced significant attenuation period may coincide with periods where no packets are captured. Although DIFFLOC only needs 5 seconds of CSI data for localization, longer capture durations generally yield better results. However, in the context of camera localization, the data throughput of video streams is sufficiently high. Human activity and multipath propagation may introduce interference. However, users have complete control over their environment, allowing them to eliminate various sources of interference. While existing WiFi camera detection methods are relatively fixed, none can guarantee the detection of all hidden cameras. Detection may also fail if the camera monitors only a small area of the room or if the user is not initially present in the monitored region. In such cases, particularly in privacy-sensitive scenarios, the user typically has control over the environment, allowing them to disable all controllable high-throughput devices and then use DIFFLOC to localize any remaining devices that continue to generate significant traffic, thereby identifying potential hidden cameras. Owing to DIFFLOC 's rapid localization capability, this process can be conducted efficiently and with minimal effort.

Multiple Cameras. While our evaluation focused on a single camera scenario, DIFFLOC can easily be extended to multiple-camera setups. During the hidden camera detection phase, a single user walking around can detect multiple cameras by clustering the MAC addresses of all sniffed packets. To localize multiple cameras, DIFFLOC would need to repeat the localization process for each camera, though this can be done without additional user effort.

Intimate Partner Violence. While DIFFLOC is primarily designed for privacy protection, we recognize that hidden WiFi cameras are also frequently used in intimate partner violence (IPV) scenarios. These situations pose unique and severe challenges: survivors often lack full control over their environment and may face significant personal risk if caught attempting to locate surveillance devices. To better support this high-risk use case, future iterations of DIFFLOC should emphasize stealth and discretion. For instance, with future access to CSI extraction from smartphone WiFi chipsets, the system could be redesigned as a compact, easy-to-assemble localization tool using only a smartphone and a small peripheral, helping to avoid suspicion and ensure safer deployment.

Extending to Other Devices. Real-world scenarios often involve other privacy-invading devices such as hidden microphones. As long as a device continuously transmits data over WiFi, DIFFLOC can theoretically localize it using the same diffraction-based principle. This makes DIFFLOC adaptable for detecting a broader range of WiFi-enabled spy devices. However, such extensions would require integration with suitable detection mechanisms. For instance, detecting a hidden microphone might involve inducing audio activity and observing corresponding changes in upload traffic to trigger localization. Extending DIFFLOC to devices using Beamforming Feedback Information (BFI) is currently infeasible, as BFI reflects the signal propagation from the camera to the access point, rather than from the camera to the monitoring device, which is the path DIFFLOC relies on.

Future Work. First, we plan to replace the current onboard antenna with an external one to enhance signal reception and mitigate interference caused by the existing hardware layout. Second, drawing on Fresnel diffraction theory, we aim to develop more robust and accurate localization models. This includes extending the current 2D framework to support 3D localization and designing optimized obstacle geometries to produce more distinctive and reliable diffraction patterns. This direction is inspired by recent work [44], which demonstrates that diffraction effects can be leveraged to reconstruct cm-level object shapes. Lastly, to address random errors and improve usability, we envision more advanced diffraction control mechanisms and search strategies tailored for real-world camera localization. For instance, implementing a reverse sweep of the obstacle could help estimate the confidence level of the localization result, allowing the system to prompt users to reposition the device for improved accuracy.

8 Conclusion

In this paper, we introduced DIFFLOC, a novel WiFi camera localization method designed to enhance privacy protection. The proposed system utilizes the diffraction phenomena of electromagnetic wave signals to localize WiFi cameras using low-cost, single-antenna COTS hardware. This approach eliminates the need for training, large spaces, and user effort, providing a robust and user-friendly solution. Experimental validation demonstrates the effectiveness of DIFFLOC in various environments and devices.

9 Ethics Considerations

The experiments in this work were conducted by the authors within their own living or working environment, ensuring that there are no ethical concerns associated with the experimental procedures. To further examine potential misuse, we simulate relevant WiFi-based attack methods in Appendix B and present a detailed case study. Our analysis shows that DIFFLOC 's through-wall localization capability is limited due to significant signal attenuation. Moreover, deploying DIFFLOC in close proximity to a victim's environment is often difficult in real-world scenarios, further reducing its potential for malicious use. Nonetheless, as camera localization systems continue to advance in precision, the associated privacy risks warrant ongoing attention. For DIFFLOC specifically, we outline several defensive strategies in Appendix B.3 aimed at mitigating potential privacy threats.

10 Open Science

We fully support the conference's policy on scientific development, as open-sourcing research allows future researchers to build upon existing work. In our own research, we frequently encountered challenges when key works were not open-sourced. Comprehensive implementation details for DIFFLOC, including code and demonstrations, are available at: https://doi.org/10.5281/zenodo.15592887, and more details please refer to Appendix D. We have provided a detailed description of the software, hardware, and operational procedures required for implementing DIFFLOC.

Acknowledgments: This work is supported by the National Key Research and Development Program of China under Grant 2022YFB3103203, the National Natural Science Foundation of China (NSFC) under the grant No.62372149, No.62462015, and No.U23A20303, the Young Elite Scientist Sponsorship Program By Gast (Grant No. GASTYESS202429) and the Key Laboratory of Knowledge Engineering with Big Data (NO. BigKEOpen2025-04).

References

[1] The security camera laws in delaware. https://www.cambasket.com/the-security-camera-laws-in-delaware/.

[2] Rose Ceccio, Sophie Stephenson, Varun Chadha, Danny Yuxing Huang, and Rahul Chatterjee. Sneaky spy devices and defective detectors: the ecosystem of intimate partner surveillance with covert devices. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 123–140, 2023.

[3] Jim Dalrymple. More than 1 in 10 airbnb guests have found hidden cameras: Survey. https://www.inman.com/2019/06/07/morethan-1-in-10-airbnb-guest-have-found-cameras-in-rentals-survey/, 2019.

[4] S. Fussell. Airbnb has a hidden-camera problem. https://www.theatlantic.com/technology/archive/2019/03/what-happens-when-youfind-cameras-your-airbnb/585007/, 2024.

[5] Andrea Goldsmith. *Wireless communications*. Cambridge university press, 2005.

[6] Francesco Gringoli, Matthias Schulz, Jakob Link, and Matthias Hollick. Free your csi: A channel state information extraction platform for modern wi-fi chipsets. In *Proceedings of the 13th International Workshop on Wireless Network Testbeds, Experimental Evaluation & Characterization*, pages 21–28, 2019.

[7] Yangyang Gu, Jing Chen, Cong Wu, Kun He, Ziming Zhao, and Ruiying Du. Loccams: An efficient and robust approach for detecting and localizing hidden wireless cameras via commodity devices. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 7(4):1–24, 2024.

[8] Yu Gu, Xiang Zhang, Yantong Wang, Meng Wang, Huan Yan, Yusheng Ji, Zhi Liu, Jianhua Li, and Mianxiong Dong. Wigrunt: Wifi-enabled gesture recognition using dual-attention network. *IEEE transactions on human-machine systems*, 52(4):736–746, 2022.

[9] Ankit Gupta. Wireless monitoring and surveillance market, by component, type, connectivity, end-user - forecast till 2030. https://www.marketresearchfuture.com/reports/wireless-monitoring-surveillance-market-975, 2024.

[10] Daniel Halperin, Wenjun Hu, Anmol Sheth, and David Wetherall. Tool release: Gathering 802.11 n traces with channel state information. *ACM SIGCOMM computer communication review*, 41(1):53–53, 2011.

[11] Yan He, Qiuye He, Song Fang, and Yao Liu. Motioncompass: pinpointing wireless camera via motion-activated traffic. In *Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services*, pages 215–227, 2021.

[12] Jeongyoon Heo, Sangwon Gil, Youngman Jung, Jinmok Kim, Donguk Kim, Woojin Park, Yongdae Kim, Kang G Shin, and Choong-Hoon Lee. Are there wireless hidden cameras spying on me? In *Proceedings of the 38th Annual Computer Security Applications Conference*, pages 714–726, 2022.

[13] Pei Huang, Xiaonan Zhang, Sihan Yu, and Linke Guo. Is-wars: Intelligent and stealthy adversarial attack to wi-fi-based human activity recognition systems. *IEEE Transactions on Dependable and Secure Computing*, 19(6):3899–3912, 2021.

[14] Global Growth Insights. Former homeland security adviser reveals how you can tell if your hotel room has a secret hidden camera. https://nypost.com/2024/03/07/tech/hidden-camera-warning-for-travelers-in-hotels-rentals-what-to-know/?utm_source=chatgpt.com, 2024.

[15] S. Jeong and J. Griffiths. Hundreds of south korean motel guests were secretly filmed and live-streamed online. https://www.cnn.com/2019/03/20/asia/southkorea-hotel-spy-cam-intl/index.html, 2019.

[16] Dawn Kawamoto. 24 iot devices connecting the world. https://builtin.com/articles/iot-devices, 2024.

[17] Changming Li, Mingjing Xu, Yicong Du, Limin Liu, Cong Shi, Yan Wang, Hongbo Liu, and Yingying Chen. Practical adversarial attack on wifi sensing through unnoticeable communication packet perturbation. In *Proceedings of the 30th Annual International Conference on Mobile Computing and Networking*, pages 373–387, 2024.

[18] Jianfeng Li, Shuohan Wu, Hao Zhou, Xiapu Luo, Ting Wang, Yangyang Liu, and Xiaobo Ma. Packet-level open-world app fingerprinting on wireless traffic. In *The 2022 Network and Distributed System Security Symposium (NDSS'22)*, 2022.

[19] Ronghua Li, Haibo Hu, and Qingqing Ye. Rftrack: Stealthy location inference and tracking attack on wi-fi devices. *IEEE Transactions on Information Forensics and Security*, 2024.

[20] Rui Li, Yu Duan, Rui Du, Fangxin Xu, Hangbin Zhao, Yang Sun, Yiyan Zhang, Daiyang Zhang, Yiming Liu, Zhiping Jiang, and Tony Xiao Han. Reshaping wifi isac with high-coherence hardware capabilities. *IEEE Communications Magazine*, 62(9):114–120, 2024.

[21] Ziwei Liu, Feng Lin, Chao Wang, Yijie Shen, Zhongjie Ba, Li Lu, Wenyao Xu, and Kui Ren. Camradar: hidden camera detection leveraging amplitude-modulated sensor images embedded in electromagnetic emanations. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 6(4):1–25, 2023.

[22] LLC LSC. Hidden camera detector. https://apps.apple.com/us/app/hidden-camera-detector/id532882360, 2023.

[23] Yongqiang Ma, Xiangyang Luo, Ruixiang Li, Shaoyong Du, and Wenyan Liu. Lenser: A channel state information based indoor localization scheme for malicious devices. In *2023 IEEE 20th International Conference on Mobile Ad Hoc and Smart Systems (MASS)*, pages 461–470. IEEE, 2023.

[24] Yongsen Ma, Gang Zhou, and Shuangquan Wang. Wifi sensing with channel state information: A survey. *ACM Computing Surveys (CSUR)*, 52(3):1–36, 2019.

[25] Xuanqi Meng, Jiarun Zhou, Xiulong Liu, Xinyu Tong, Wenyu Qu, and Jianrong Wang. Secur-fi: A secure wireless sensing system based on commercial wi-fi devices. In *IEEE INFOCOM 2023-IEEE Conference on Computer Communications*, pages 1–10. IEEE, 2023.

[26] Metageek. The basics: Understanding rssi. https://www.metageek.com/training/resources/understanding-rssi/, 2019.

[27] Ben Nassi, Raz Ben-Netanel, Adi Shamir, and Yuval Elovici. Drones' cryptanalysis-smashing cryptography with a flicker. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 1397–1414. IEEE, 2019.

[28] FOX News. Wifi chipsets market size, share, groeth, and industry analysis, by types. https://www.globalgrowthinsights.com/market-reports/wi-fi-chipsets-market-111160, 2025.

[29] Jorge Ortiz, Catherine Crawford, and Franck Le. Devicemien: network device behavior modeling for identifying unknown iot devices. In *Proceedings of the International Conference on Internet of Things Design and Implementation*, pages 106–117, 2019.

[30] Zhaoqing Pan, Jianjun Lei, Yun Zhang, Xingming Sun, and Sam Kwong. Fast motion estimation based on content property for low-complexity h. 265/hevc encoder. *IEEE Transactions on Broadcasting*, 62(3):675–684, 2016.

[31] Theodore S Rappaport. *Wireless communications: principles and practice*. Cambridge University Press, 2024.

[32] Sriram Sami, Sean Rui Xiang Tan, Bangjie Sun, and Jun Han. Lapd: Hidden spy camera detection using smartphone time-of-flight sensors. In *Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems*, pages 288–301, 2021.

[33] Matthias Schulz, Daniel Wegemer, and Matthias Hollick. Nexmon: The c-based firmware patching framework. https://nexmon.org, 2017.

[34] Rahul Anand Sharma, Elahe Soltanaghaei, Anthony Rowe, and Vyas Sekar. Lumos: Identifying and localizing diverse hidden {IoT} devices in an unfamiliar environment. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 1095–1112, 2022.

[35] Akash Deep Singh, Luis Garcia, Joseph Noor, and Mani Srivastava. I always feel like somebody's sensing me! a framework to detect, identify, and localize clandestine wireless sensors. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 1829–1846, 2021.

[36] Arunan Sivanathan, Hassan Habibi Gharakheili, Franco Loi, Adam Radford, Chamith Wijenayake, Arun Vishwanath, and Vijay Sivaraman. Classifying iot devices in smart environments using network traffic characteristics. *IEEE Transactions on Mobile Computing*, 18(8):1745–1759, 2018.

[37] Jakobi Teknik. Spy hidden camera detector. https://apps.apple.com/us/app/spy-hidden-cameradetector/id925967783?mt=8, 2023.

[38] Geert Van der Auwera, Prasanth T David, and Martin Reisslein. Traffic characteristics of h. 264/avc variable bit rate video. *IEEE Communications Magazine*, 46(11):164–174, 2008.

[39] Mathy Vanhoef, Célestin Matte, Mathieu Cunche, Leonardo S Cardoso, and Frank Piessens. Why mac address randomization is not enough: An analysis of wi-fi network discovery mechanisms. In *Proceedings of the 11th ACM on Asia conference on computer and communications security*, pages 413–424, 2016.

[40] Christopher Wampler, Selcuk Uluagac, and Raheem Beyah. Information leakage in encrypted ip video traffic. In *2015 IEEE Global Communications Conference (GLOBECOM)*, pages 1–7. IEEE, 2015.

[41] Xuanzhi Wang, Kai Niu, Jie Xiong, Bochong Qian, Zhiyun Yao, Tairong Lou, and Daqing Zhang. Placement matters: Understanding the effects of device placement for wifi sensing. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 6(1):1–25, 2022.

[42] Xuanzhi Wang, Anlan Yu, Kai Niu, Weiyan Shi, Junzhe Wang, Zhiyun Yao, Rahul C Shah, Hong Lu, and Daqing Zhang. Understanding the diffraction model in static multipath-rich environments for wifi sensing system design. *IEEE Transactions on Mobile Computing*, 2024.

[43] Rui Xiao, Xiankai Chen, Yinghui He, Jun Han, and Jinsong Han. Lend me your beam: Privacy implications of plaintext beamforming feedback in wifi. In *NDSS*, 2025.

[44] Zhiyun Yao, Xuanzhi Wang, Kai Niu, Rong Zheng, Junzhe Wang, and Daqing Zhang. Wiprofile: Unlocking diffraction effects for sub-centimeter target profiling using commodity wifi devices. In *Proceedings of the 30th Annual International Conference on Mobile Computing and Networking*, pages 185–199, 2024.

[45] Zhiyuan Yu, Zhuohang Li, Yuanhaur Chang, Skylar Fong, Jian Liu, and Ning Zhang. Heatdecam: detecting hidden spy cameras via thermal emissions. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, pages 3107–3120, 2022.

[46] Fusang Zhang, Kai Niu, Jie Xiong, Beihong Jin, Tao Gu, Yuhang Jiang, and Daqing Zhang. Towards a diffraction-based sensing approach on human activity recognition. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 3(1):1–25, 2019.

[47] Fusang Zhang, Daqing Zhang, Jie Xiong, Hao Wang, Kai Niu, Beihong Jin, and Yuxiang Wang. From fresnel diffraction model to fine-grained human respiration sensing with commodity wi-fi devices. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, 2(1), mar 2018.

[48] Qibo Zhang, Daibo Liu, Xinyu Zhang, Zhichao Cao, Fanzi Zeng, Hongbo Jiang, and Wenqiang Jin. Eye of sauron:{Long-Range} hidden spy camera detection and positioning with inbuilt memory {EM} radiation. In *33rd USENIX Security Symposium (USENIX Security 24)*, pages 109–126, 2024.

[49] Xianan Zhang, Wei Wang, Xuedou Xiao, Hang Yang, Xinyu Zhang, and Tao Jiang. Peer-to-peer localization for single-antenna devices. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 4(3):1–25, 2020.

[50] Xiang Zhang, Yu Gu, Huan Yan, Yantong Wang, Mianxiong Dong, Kaoru Ota, Fuji Ren, and Yusheng Ji. Wital: A cots wifi devices based vital signs monitoring system using nlos sensing model. *IEEE Transactions on Human-Machine Systems*, 53(3):629–641, 2023.

[51] Xiang Zhang, Jinyang Huang, Huan Yan, Yuanhao Feng, Peng Zhao, Guohang Zhuang, Zhi Liu, and Bin Liu. Wiopen: A robust wi-fi-based open-set gesture recognition framework. *IEEE Transactions on Human-Machine Systems*, 55(2):234–245, 2025.

[52] Xiang Zhang, Jie Zhang, Zehua Ma, Jinyang Huang, Meng Li, Huan Yan, Peng Zhao, Zijian Zhang, Bin Liu, Qing Guo, Tianwei Zhang, and NengHai Yu. Camlopa: A hidden wireless camera localization framework via signal propagation path analysis. In *2025 IEEE Symposium on Security and Privacy (SP)*, pages 3653–3671, Los Alamitos, CA, USA, May 2025.

[53] Yanzi Zhu, Zhujun Xiao, Yuxin Chen, Zhijing Li, Max Liu, Ben Y Zhao, and Heather Zheng. Et tu alexa? when commodity wifi devices turn into adversarial motion sensors. In *Proceedings 2020 Network and Distributed System Security Symposium*. Internet Society, 2020.

[54] Agustin Zuniga, Naser Hossein Motlagh, Mohammad A Hoque, Sasu Tarkoma, Huber Flores, and Petteri Nurmi. See no evil: Discovering covert surveillance devices using thermal imaging. *IEEE Pervasive Computing*, 21(4):33–42, 2022.

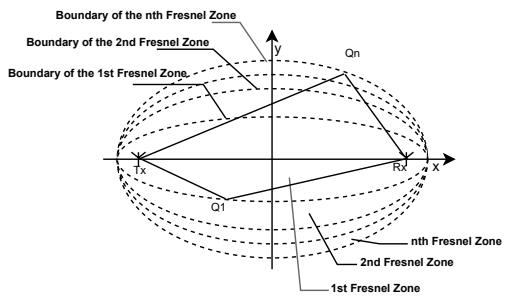


Figure 15: Illustration of Fresnel Zone.

A Fresnel Zone Visualization

The visualization of the Fresnel zones is shown in Figure 15, consisting of a series of concentric ellipses.

B Ethical Case Study: Privacy Tracking

B.1 Threat Model

We focus on a scenario in which an attacker leverages WiFi signals emitted by a user's indoor devices to infer their presence, behaviors, and daily routines for malicious purposes. For example, the attacker may first use WiFi-based localization techniques from outside the user's room to determine the spatial layout of various devices. Then, by passively monitoring the traffic and CSI from these devices, the attacker can infer whether the user is nearby and analyze their usage habits. Such information could be exploited for targeted burglaries or stalking [43]. In this paper, the goal of this analysis is not to propose new attacks but to raise awareness of how advances in camera localization could enable privacy intrusions.

- To remain stealthy, the attacker does not actively probe the environment. Instead, they passively sniff WiFi traffic and CSI from outside the target area, without any cooperation from the victim's devices or the need to inject packets.
- The attacker leverages DIFFLOC and a triangulation-based method to determine the positions of devices within the room. Once localized, variations in CSI can be analyzed to detect whether the user is near a specific device and to infer activity patterns over time for malicious purposes.
- The attacker must be close to the target environment, such as in an adjacent apartment. WiFi signals experience significant attenuation when passing through walls, which limits the effectiveness of this side-channel attack.

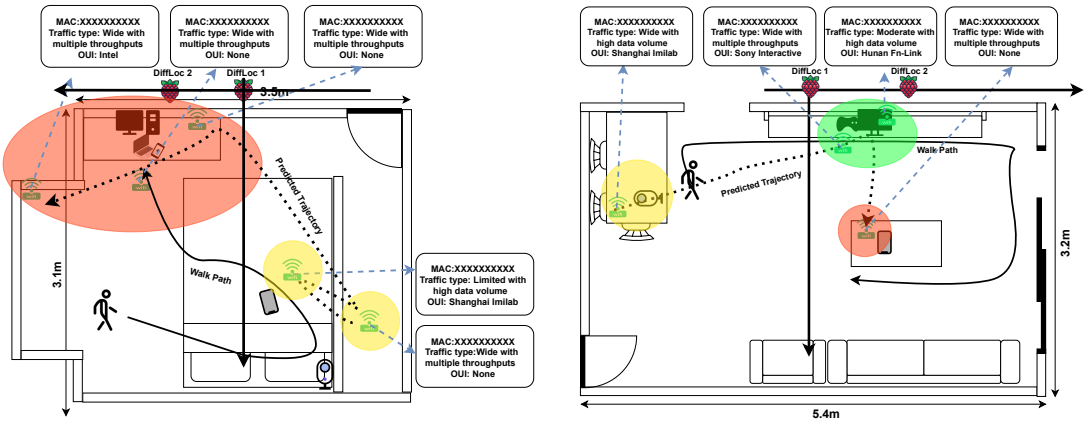
B.2 Method

In this section, we present the privacy tracking method built on DIFFLOC to demonstrate the potential risks posed by DIFFLOC. Following previous studies [19, 53], we begin by scanning for all APs in the environment and identifying the target AP based on signal strength and name. The privacy tracking process starts by sniffing traffic from the channel of the target AP. The collected traffic is then clustered based on MAC addresses, and the corresponding MAC addresses and WiFi channels are passed to DIFFLOC for localization. For device localization, DIFFLOC is deployed at two different positions to estimate the target device's azimuth angle. Triangulation is then applied to determine the final position of the target. The privacy information is then extracted through a combination of MAC address analysis, traffic analysis, and CSI analysis. DIFFLOC collects CSI from multiple devices by hopping between MAC addresses.

From the MAC address and traffic data, we use the Organizationally Unique Identifier (OUI) in the MAC address to identify the manufacturer of each device and analyze the diversity of traffic types and data throughput. We classify traffic into four models: stable, continuous high-speed upload (e.g., camera); stable, continuous high-speed download (e.g., live streaming or downloading); stable low-speed traffic (e.g., prolonged web browsing); and fluctuating high-speed download (e.g., video streaming). Devices exhibiting only one traffic type are classified as limited; two types are classified as moderate; and three to four types are classified as wide. For CSI analysis, we assess fluctuations in the signal to detect potential human activity near the target device. Human activity often causes reflection and diffraction of the WiFi signal, leading to corresponding fluctuations in the CSI. However, significant impacts on CSI are only observed when activity occurs close to the device [41]. Thus, we interpret these significant fluctuations as indicators that a monitored subject may be nearby. By analyzing a user's presence at different locations, we can infer their live trajectory and the frequency of their activity.

B.3 Analysis of Ethical Risk

Rooms 1 and 3 were used for evaluation. In these rooms, various WiFi devices were deployed based on the functional



(a) Privacy tracking in Room1

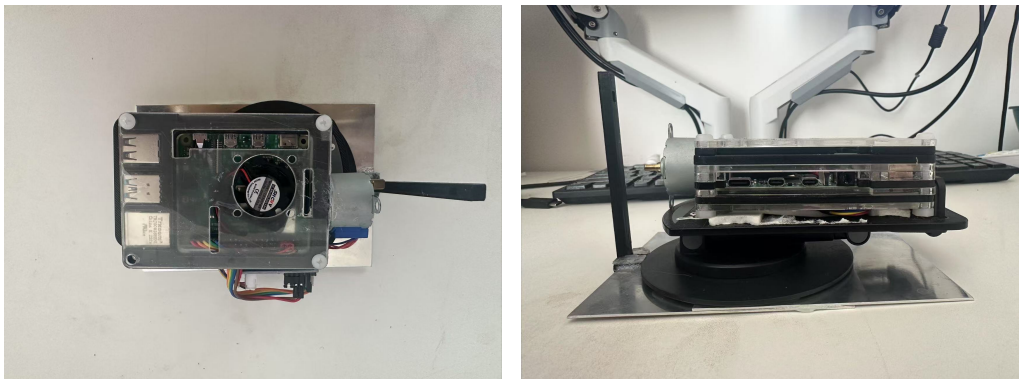
(b) Privacy tracking in Room3

Figure 16: Privacy tracking in Room 1 and 3. The locations and types of WiFi devices are represented by corresponding icons, while the victim's live trajectory is indicated by solid arrows and the predicted trajectory by dashed arrows.

differences of each environment. As shown in Figure 16, Room 1 serves as a space for daily work and living, equipped with a desktop computer, MacBook, two smartphones (Android and iPhone), and a surveillance camera. Room 3 is the living room, which includes a PS5 game console, television, WiFi surveillance camera, and an iPhone. DIFFLOC is placed outside each room, positioned through the wall. For Room 1, the distance between the two DIFFLOC devices is 1 meter, while for Room 3, it is 1.35 meters. During evaluation, participants simulated typical daily activities, moving through different areas where the WiFi devices were located, following a predefined path. Participants also used each device for typical network activities.

As shown in Figure 16, the localization results, for each device are marked with green WiFi device locations. Manufacturer information and traffic types for each device are provided in labeled boxes, and ellipses in three different colors represent the frequency of user activity around each device: red, yellow and green indicate high, moderate, and low activity frequency, respectively. During our evaluation, the OUI of cameras and PS5 consoles successfully revealed the manufacturer, while for devices such as smartphones and MacBooks, the manufacturer could not be identified. This is likely due to MAC address randomization, a technique used to enhance device privacy. In Room 1, frequent activity in the upper-left corner, where several wide traffic type devices are located, suggests that this may be the user's desk. In both Rooms 1 and 3, the system effectively tracks the user's living trajectory, including transitions between different areas, and provides approximate locations of these areas. This information can be valuable for monitoring daily activities and extracting other privacy-related insights. The average localization error of our system in privacy tracking is 0.86 meters. Compared to previous room-level attacks [53], the results show that the DIFFLOC-based system can reveal sub-room-level privacy information.

As the above analysis shows, DIFFLOC 's localization capability remains limited in through-wall scenarios. Combined with the inherent complexity of real-world environments and the challenges of deploying the system in close proximity to residential rooms, its potential for malicious use is further constrained. Nevertheless, it is important to recognize that systems originally designed for locating hidden cameras could be repurposed for malicious applications. This potential risk underscores the importance of ethical design and deployment of such systems, a consideration that is often overlooked in current similar studies. To mitigate potential privacy risks, we also propose several strategies. First, WiFi device manufacturers could introduce controlled random noise into CSI to mitigate the effectiveness of CSI-based side-channel attacks. However, this would require widespread industry adoption and proactive efforts from manufacturers, which may be challenging to implement. As noted earlier, modifying the network behavior of purchased WiFi devices is difficult for individual users. Second, users can minimize privacy leakage by positioning high-throughput devices as far as possible from areas with frequent human activity. Additionally, placing high-throughput devices can increase DIFFLOC's localization error due to co-channel interference, as shown in Figure 16a. Third, users may deploy active co-channel signals, such as Zigbee or WiFi injection, to disrupt indoor multipath propagation, introducing significant noise into the CSI. These methods have been partially validated [13, 17, 25]. These techniques require moderate-sized equipment and a continuous power supply, making them impractical for attackers to use as a means of disabling camera localization systems.



(a) Top view (b) Side view

Figure 17: The folded DIFFLOC system.

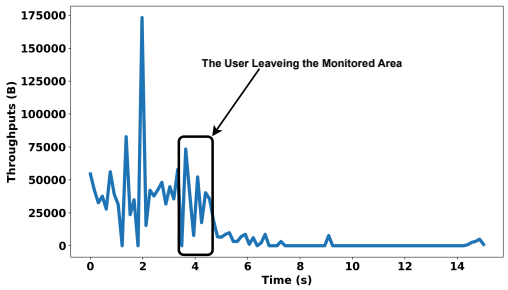


Figure 18: Throughput during the user's exit from the room.

C More Details of Camera Detection

Video use three types of frames to compress video:

- I (Intra-coded) frames: These frames contain complete image data and can be decoded independently of other frames.
- P (Predicted) frames: These frames encode residual information and rely on preceding I frames for decoding.
- B (Bi-directionally predicted) frames: These frames generate images by referencing preceding I or P frames, subsequent I or P frames, or interpolations between them.

Among these frame types, B frames are the most compressible, followed by P frames, with I frames being the least compressible. In video footage captured by the camera, significant changes between frames lead to an increase in the number of P and B frames, which in turn results in higher upload traffic. This means that when there is user activity, the wireless camera transmits more data. Figure 18 illustrates the variation in camera traffic when a user leaves the monitored area, clearly showing a sharp decrease in traffic after the user departs.

D Implementation of Prototype

DIFFLOC requires sniffing 802.11 packets to obtain CSI. Currently, most mobile devices require special permissions for packet sniffing, and due to the closed-source nature of wireless network card manufacturers, CSI extraction is only possible with certain models. While obtaining CSI is not technically challenging, it depends on whether access and control permissions are granted by the manufacturer. To ensure broad applicability and future scalability, we chose not to implement DIFFLOC on a specific smartphone or computer platform that supports CSI extraction. Instead, we selected the Raspberry Pi, a low-cost, open-source, COTS device, as the platform.

Our implementation, code, and demo are available at: https://github.com/CamLoPA/DiffLoc. The DIFFLOC prototype is built on the Raspberry Pi 4B, running Raspberry Pi OS with kernel version 4.9 and firmware version 7_45_189. The code is implemented using Python 3. The stepper motor used is the 28BYJ-48 model, controlled by a ULN2003 board. Before using the DIFFLOC, users must install the nexmoncsi tool and the required Python dependencies. It is important to avoid using the upgrade commands during setup, as updating the firmware may cause nexmoncsi to malfunction. Additionally, since this system version is older and no longer maintained, some packages must be installed via the apt-get command rather than pip. During the installation of nexmoncsi, wireless network functionality is temporarily disabled. Users must manually activate the wireless interface and configure the network settings.

E Portability

The folded DIFFLOC system, as shown in Figure 17, is only slightly larger than a standard Raspberry Pi, making it highly portable and easy to carry. This folding structure uses a mechanism similar to COTS phone stands, making it intuitive and easy for users to fold correctly.