Hidden WiFi Camera Localization via Signal Propagation Path Analysis

Xiang Zhang[†*], Zehua Ma[†*], Jingyang Huang[$✉], Huan Yan[#], Meng Li[$], Zhi Liu[‡], and Bin Liu[†✉]

[†]University of Science and Technology of China, China, [$]Hefei University of Technology, China, [#]Guizhou Normal University, China, [‡]The University of Electro-Communications, Japan,[✉]: Corresponding authors.

ABSTRACT

Hidden WiFi cameras pose significant privacy threats, necessitating effective localization methods. In this work, we introduce CamLoPA, a system designed for the detection and localization of WiFi cameras. CamLoPA achieves this in just 45 seconds of user walking. It begins by analyzing the causal relationship between WiFi traffic and user movement to identify the presence of a snooping camera. Upon detection, CamLoPA utilizes a novel azimuth location model based on WiFi signal propagation path analysis to localize the hidden camera. Comprehensive evaluations demonstrate that CamLoPA can accurately and swiftly detect and localize snooping WiFi cameras with minimal constraints.

CCS CONCEPTS

• **Security and privacy** → **Privacy protections**.

KEYWORDS

Camera Detection, WiFi Camera, CSI, Camera Loclization

ACM Reference Format:
Xiang Zhang[†*], Zehua Ma[†*], Jingyang Huang[$✉], Huan Yan[#], Meng Li[$], Zhi Liu[‡], and Bin Liu[†✉]. 2024. Hidden WiFi Camera Localization via Signal Propagation Path Analysis. In . ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

In recent years, the widespread adoption of WiFi cameras for home and public security has surged, owing to their convenience and flexible deployment. However, this rapid proliferation has also heightened privacy concerns regarding unauthorized video recording and dissemination. Increasingly, users are illegally recorded by hidden cameras in various locations, from hotel rooms to short-term rentals [3]. This underscores the urgent need for effective methods to detect and localize hidden WiFi cameras [2, 4, 5].

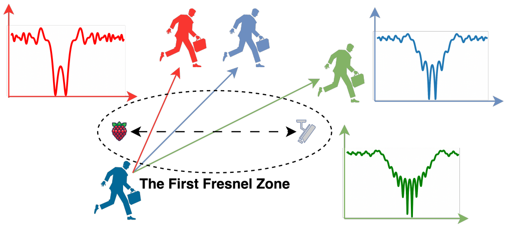


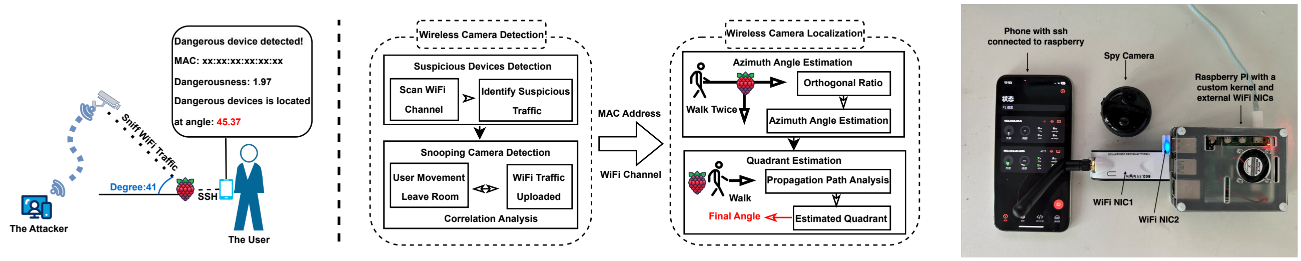
Figure 1: Path losses when crossing the FFZ.

In this paper, we introduce CamLoPA, a fast and robust WiFi camera detection and localization framework using low-cost commercial-off-the-shelf (COTS) devices. Our framework is inspired by the relationship between obstructions in the propagation path of WiFi signals and the resulting signal attenuation. Specifically, when a large obstacle is located within the First Fresnel Zone (FFZ) between a WiFi transmitter and receiver, the transmitted signal will experience significant attenuation due to diffraction [6–8]. As illustrated in Figure 1, when a person crosses the FFZ, there is a drastic change in the WiFi signal path loss (can be represented by Channel State Information(CSI)), and the duration of this significant variation is related to the length of the path traversed through the FFZ. Since the FFZ forms an ellipse with the two devices as its foci, given a fixed distance between the two devices and the know user's body size, the length of the path through the FFZ can be mapped to the angle of the walk relative to the LOS path (**azimuth**). CamLoPA utilizes this relationship to develop a azimuth localization model and achieve azimuth estimation of the snooping WiFi camera.

However, there are two significant challenges: ***1) Unknown User Speed*** and ***2) Unknown Distance Between Devices and User Body Size.*** We can only determine the time of significant attenuation from the CSI. Consequently, the first challenge prevents us from obtaining the path length,

Conference'17, July 2017, Washington, DC, USA

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM
https://doi.org/10.1145/nnnnnnn.nnnnnnn



(a) Overview.

(b) Prototype

Figure 2: The Overview and Prototype of CamLoPA.

making it impossible to establish a relationship between path length and azimuth. The latter challenge implies that distance and body size must be predefined, introducing considerable errors into the established mapping. To address these challenges, we propose a scheme called the ***orthogonal ratio***. This approach replaces the need to measure the distance of a single path through the FFZ with *the time ratio of two orthogonal paths crossing the FFZ* to establish a mapping relationship with the azimuth angle. We implement a prototype of CamLoPA on a Raspberry Pi 4B device.

2 SYSTEM DESIGN

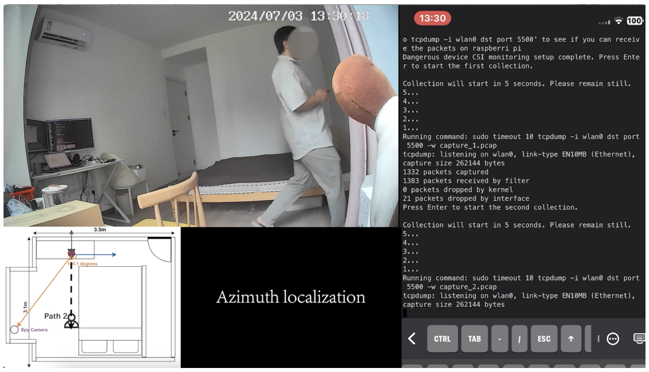
The overall structure of CamLoPA is shown in Figure 2(a) and operates in two phases:

Hidden WiFi Camera Detection. CamLoPA first scans the surrounding WiFi networks and captures packets on all active 802.11 WiFi channels to identify suspicious devices that continuously upload data. The snooping camera detection module then prompts the user to leave the room and sniffs packets from the identified channel for 15 seconds. If the traffic pattern matches the user's departure phase, the module reports the presence of a snooping camera.

Hidden WiFi Camera Localization. Once a snooping camera is detected, CamLoPA prompts the user to walk along two orthogonal paths intersecting the CamLoPA device. The device sniffs the WiFi packets transmitted from the camera over 10 seconds for each path, extracting CSI to calculate the orthogonal ratio and determine the azimuth angle using the proposed azimuth localization model. After calculating the azimuth angle, CamLoPA prompts the user to walk along a path coinciding with the first path but starting in front of the CamLoPA device, collecting 10 seconds of CSI. Finally, using the quadrant determination model, CamLoPA estimates the quadrant in which the target device is located to obtain the final azimuth angle of the hidden WiFi camera.

3 DEMONSTRATION

The prototype of CamLoPA is shown in Figure 2(b). The Pi4 utilizes its built-in wireless NIC with the nexmon tool [1] to modify the kernel for CSI extraction. We set up an external network card (NIC1) with monitoring capabilities to sniff 802.11 packets, while NIC2 is a standard wireless network card used for communication. The demo of CamLoPA is shown in Figure 3. The user's smartphone receives prompts and localization results from CamLoPA via SSH tools. The top left shows the real environment (a bedroom), while the bottom left provides a schematic diagram and phase descriptions. The right side displays the user's smartphone interface. During the detection phase, CamLoPA prompts the user to leave the room and check for the presence of any snooping cameras. In the localization phase, CamLoPA guides the user through three walking sequences via command line prompts to locate the camera. The final localization results are displayed on the user's mobile screen via SSH. The demo is available at https://youtu.be/GKam04FzeM4. We also evaluated the performance of CamLoPA on seven different wireless cameras across three environments. Specifically, the environments included a spacious living room, a moderately open bedroom, and a crowded bedroom. The cameras had transmission rates ranging from 35 to 130 packets per second and were deployed at 4 to 6 different locations within each room. The evaluation resulted in a 95.37% detection accuracy and an average localization error of 17.46°.



```
o tcpdump -i wlan0 dst port 5500' to see if you can receiv
e the packets on raspberri pi
Dangerous device CSI monitoring setup complete. Press Ente
r to start the first collection.

Collection will start in 5 seconds. Please remain still.
5...
4...
3...
2...
1...
Running command: sudo timeout 10 tcpdump -i wlan0 dst port
 5500 -w capture_1.pcap
tcpdump: listening on wlan0, link-type EN10MB (Ethernet),
capture size 262144 bytes
1332 packets captured
1383 packets received by filter
0 packets dropped by kernel
21 packets dropped by interface
Press Enter to start the second collection.

Collection will start in 5 seconds. Please remain still.
5...
4...
3...
2...
1...
Running command: sudo timeout 10 tcpdump -i wlan0 dst port
 5500 -w capture_2.pcap
tcpdump: listening on wlan0, link-type EN10MB (Ethernet),
capture size 262144 bytes
```

Figure 3: The Demo of CamLoPA.

REFERENCES

[1] Francesco Gringoli, Matthias Schulz, Jakob Link, and Matthias Hollick. 2019. 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*. 21–28.

[2] Yangyang Gu, Jing Chen, Cong Wu, Kun He, Ziming Zhao, and Ruiying Du. 2024. 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 (2024), 1–24.

[3] Ankit Gupta. 2024. Wireless Monitoring and Surveillance Market, by Component, Type, Connectivity, End-User - Forecast till 2030. https://www.marketresearchfuture.com/reports/wireless-monitoring-surveillance-market-975.

[4] Rahul Anand Sharma, Elahe Soltanaghaei, Anthony Rowe, and Vyas Sekar. 2022. Lumos: Identifying and localizing diverse hidden IoT devices in an unfamiliar environment. In *USENIX Security 22*. 1095–1112.

[5] Akash Deep Singh, Luis Garcia, Joseph Noor, and Mani Srivastava. 2021. 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)*. 1829–1846.

[6] Xuanzhi Wang, Anlan Yu, Kai Niu, Weiyan Shi, Junzhe Wang, Zhiyun Yao, Rahul C Shah, Hong Lu, and Daqing Zhang. 2024. Understanding the Diffraction Model in Static Multipath-Rich Environments for WiFi Sensing System Design. *IEEE Transactions on Mobile Computing* (2024).

[7] Fusang Zhang, Kai Niu, Jie Xiong, Beihong Jin, Tao Gu, Yuhang Jiang, and Daqing Zhang. 2019. Towards a diffraction-based sensing approach on human activity recognition. *IMWUT/Ubicomp* 3, 1 (2019), 1–25.

[8] Xiang Zhang, Yu Gu, Huan Yan, Yantong Wang, Mianxiong Dong, Kaoru Ota, Fuji Ren, and Yusheng Ji. 2023. Wital: A COTS WiFi Devices Based Vital Signs Monitoring System Using NLOS Sensing Model. *IEEE Transactions on Human-Machine Systems* 53, 3 (2023), 629–641.