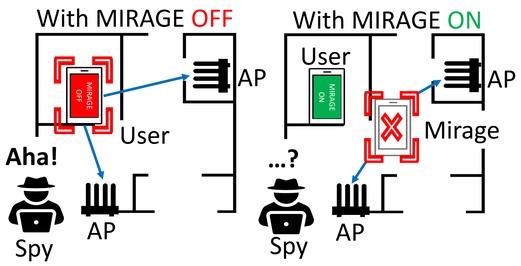
Users are Closer than They Appear: Protecting User Location from WiFi APs

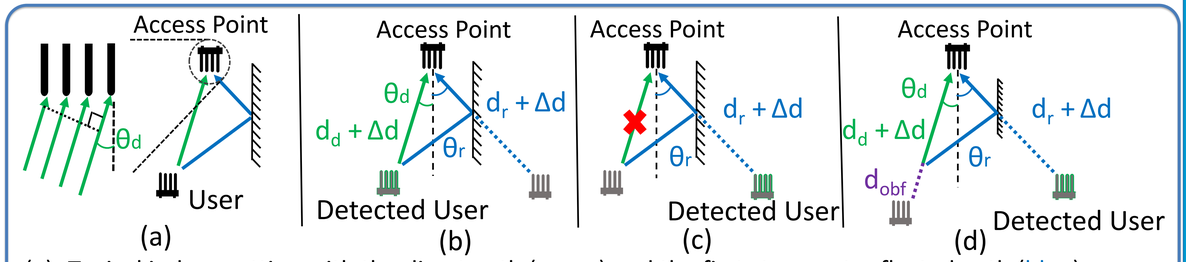
Roshan Ayyalasomayajula, Aditya Arun, Wei Sun, Dinesh Bharadia
Electrical and Computer Engineering, UC San Diego
Contact: Dinesh B. (dineshb@ucsd.edu), Roshan A. (roshana@ucsd.edu)

Motivation



- **(*Left*)** Users are exposed in wireless space. The spy can easily localize user's location with wireless sensing techniques
- **(*Right*)** *MIRAGE* protects user location from WiFi APs without interrupting the on-going wireless communication

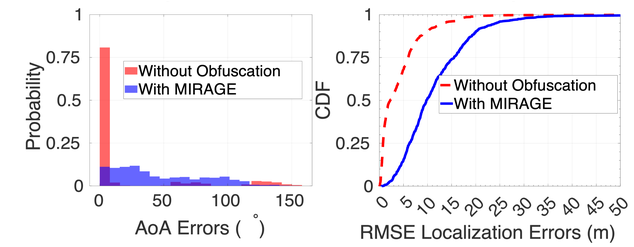
Key Idea



(a) Typical indoor setting with the direct path (green) and the first strongest reflected path (blue)
(b) AP can estimate the angle of arrivals (AoAs) to be {θ_d, θ_r} and the relative time of flights (rToFs) as {$d_d+\Delta d$, $d_r+\Delta d$} ($d_d<d_r$). Direct path AoA θ_d is chosen as it arrives earliest.
(c) When the user does beam nulling to the direct path, AP will incorrectly estimate AoA at the cost of reduced SNR
(d) When the user adds extra delay to the direct path and makes $d_d + d_{obf} > d_r$, the estimated AoA is θ_r as reflected path seems to arrive earlier. No SNR reduction is observed as direct path is preserved.

Results

Feasibility of MIRAGE – Incorrect AoA is predicted



PDF of AoA errors

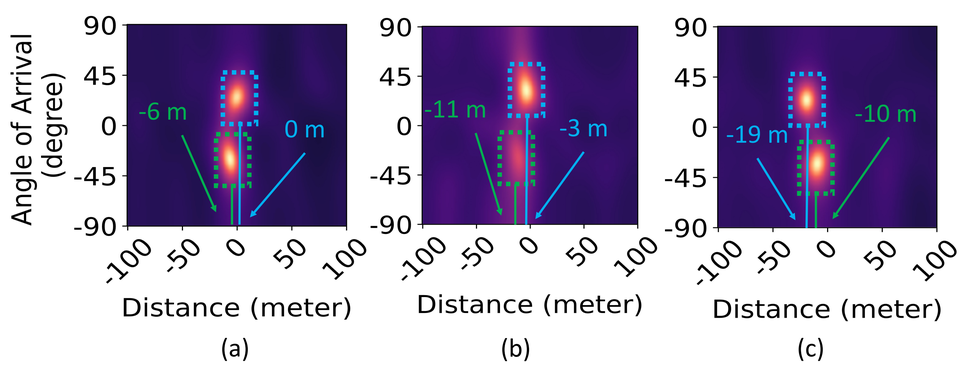
CDF of RMSE localization errors

MIRAGE will not affect the wireless communication

	No obf.	Nulling	MIRAGE with delay of			
			0 (m)	20 (m)	30 (m)	40(m)
AoA error	0^o	62^o	0^o	58^o	61^o	53^o
RSSI (dBm)	-65	-71	-64	-64	-64	-62

AoA error and RSSI measured without obfuscation, with nulling, and using MIRAGE to delay the path by varying amounts. RSSI does not degrade with MIRAGE

MIRAGE



(a) Angle-distance profiles representing the direct path and reflected path angle of arrivals and their relative distance travelled measured from COTS AP. The direct path is at -6m and reflected path is at 0m.
(b) When the user applies the beam nulling to the direct path, SpotFi will incorrectly identify the reflected path at -3m as the direct path.
(c) When the user beamforms to the direct path and adds extra delay of 15m to it, SpotFi will incorrectly identify the reflected path as the direct path.

Related Work

(a) MAC address randomization, defences against FTM /signal strength

- MAC address randomization is easy to be broken [1],
- Signal-strength based obfuscation interrupts the on-going wireless communication [2]
- FTM based localization [3] can be leveraged for privacy invasive localization.

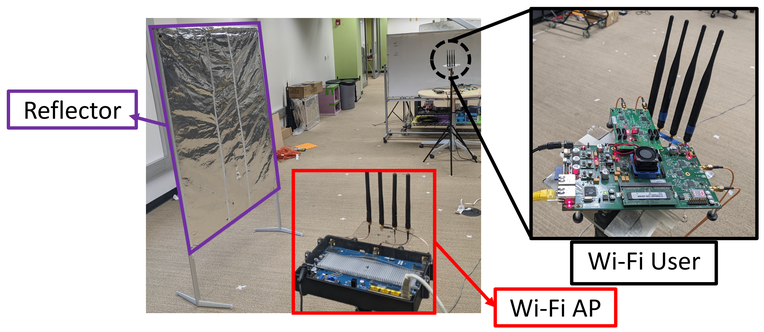
(b) Modifying the wireless environment

PhyCloak[4], IRShield [5], RF-Protect [6] and Aegis [7] try to modify the wireless environment but interrupt the ongoing wireless communication or require extra hardware deployment

[1]C. Matte and M. Cunche. Spread of MAC address randomization studied using locally administered MAC addresses use historic. PhD thesis, Inria Grenoble Rhône-Alpes, 2018.
[2]Y. Zhu, Z. Xiao, Y. Chen, Z. Li, M. Liu, B. Y. Zhao, and H. Zheng. Et tu alexa? when commodity wifi devices turn into adversarial motion sensors. arXiv preprint arXiv:1810.10109, 2018
[3] A. Abedi and D. Vasisht. Non-cooperative wi-fi localization & its pri- vacy implications. In Proceedings of the 28th Annual International Con- ference On Mobile Computing And Networking, pages 126–138. ACM, 2022.
[4]Y. Qiao, O. Zhang, W. Zhou, K. Srinivasan, and A. Arora. {PhyCloak}: Obfuscating sensing from communication signals. In 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16), pages 685–699, 2016.
[5] P. Staat, S. Mulzer, S. Roth, V. Moonsamy, M. Heinrichs, R. Kronberger, A. Sezgin, and C. Paar. Irshield: A countermeasure against adversarial physical-layer wireless sensing. In 2022 IEEE Symposium on Security and Privacy (SP), pages 1705–1721. IEEE, 2022.
[6] J. Shenoy, Z. Liu, B. Tao, Z. Kabelac, and D. Vasisht. Rf-protect: pri- vacy against device-free human tracking. In Proceedings of the ACM SIGCOMM 2022 Conference, pages 588–600, 2022.
[7] Y. Yao, Y. Li, X. Liu, Z. Chi, W. Wang, T. Xie, and T. Zhu. Aegis: An interference-negligible rf sensing shield. In IEEE INFOCOM 2018-IEEE conference on computer communications, pages 1718–1726. IEEE, 2018.

SCAN ME

Experimental Setup



Hardware: Hardware setup showcasing the ASUS WiFi-AP, WARP client and reflector in a typical indoor environment. There are mainly two paths between WiFi AP and WiFi user: direct path and the reflected path reflected off the reflector.
Software: The WiFi AP and WiFi user will communicate with each other with 802.11n protocol. WiFi user generate 802.11n packets, which will be transmitted using WARP. ASUS WiFi AP will receive these packets. MIRAGE is applied at the WiFi user and SpotFi is running at the WiFi AP.
Experimental settings: We do experiments in a typical indoor environments shown in the left figure.