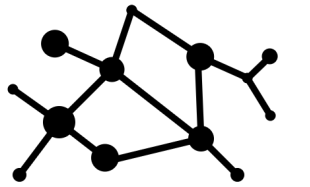
UC San Diego
JACOBS SCHOOL OF ENGINEERING
Electrical and Computer Engineering

HotMobile 2023 Orange County California



WCSNG
Wireless Communications Sensing and Networking

Users are closer than they appear

MIRAGE: Protecting User Locations from Wi-Fi APs

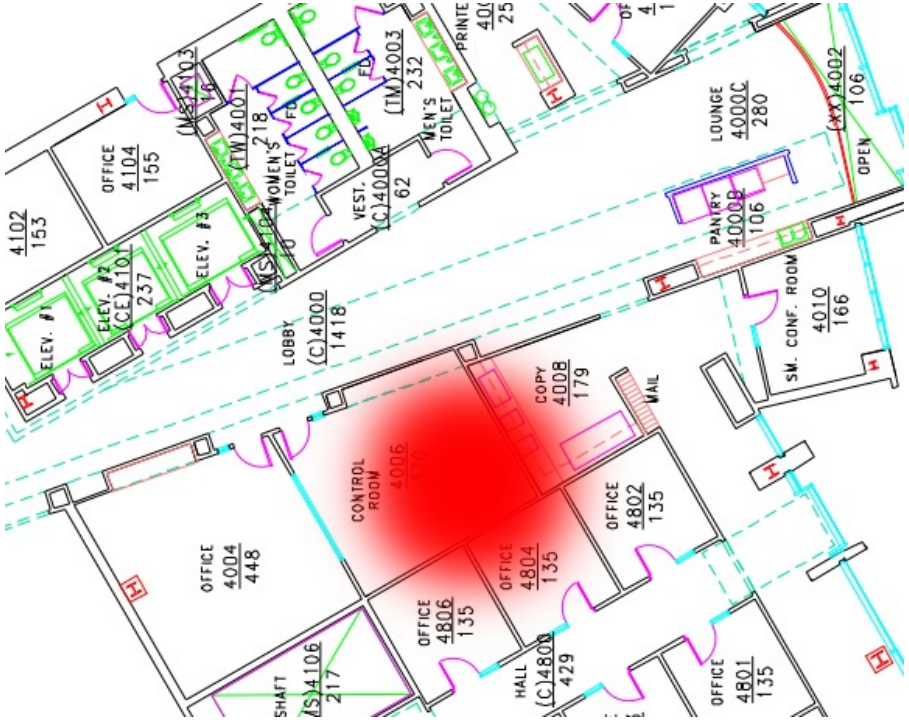
Roshan Ayyalasomayajula*, Wei Sun*, Aditya Arun*

Dinesh Bharadia

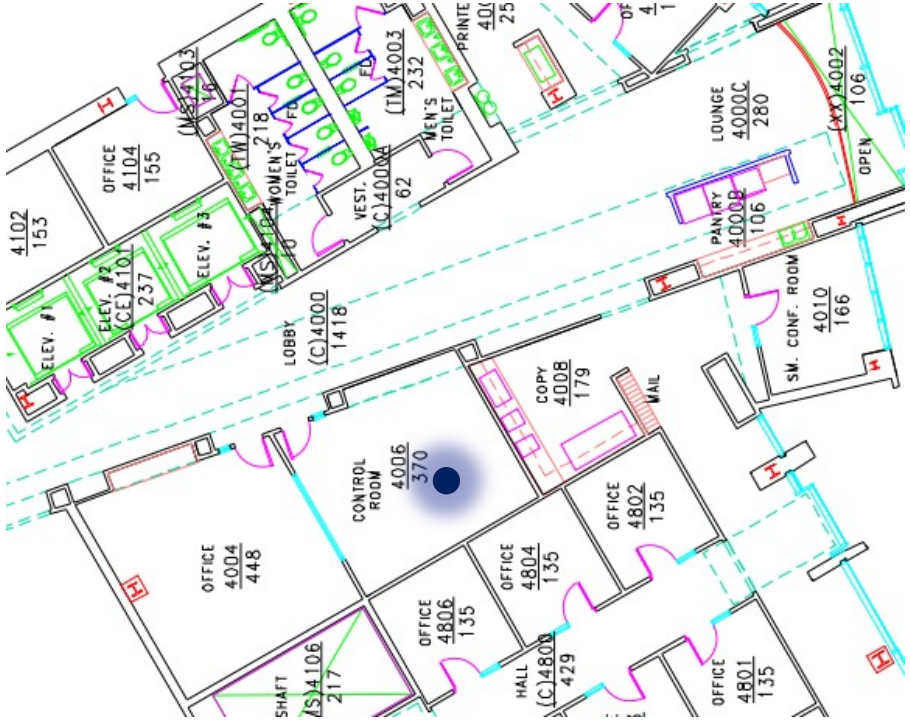
* co-primary

Wi-Fi based Localization over the years

Signal Strength Based

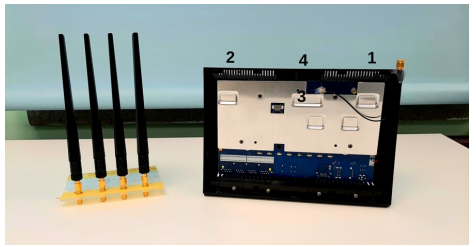


State of the art



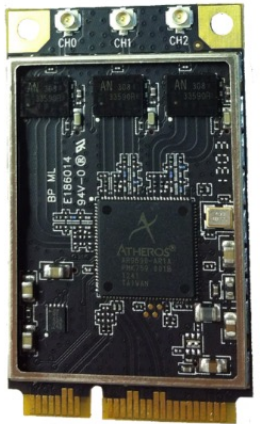
Location as a Service is now a commonplace

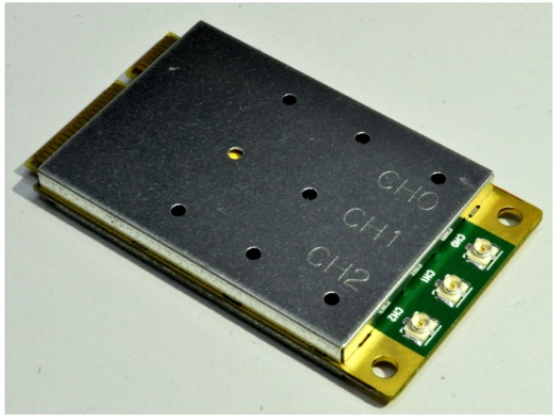
Location as a Service is now a commonplace



NEXMON CSI Tool
ASUS RT-AC86U

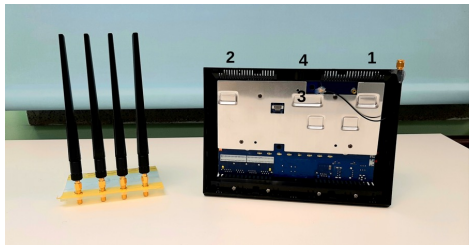
Intel-PicoScenes
Intel AX200, IWL 5300, QCA9300, SDRs





Atheros CSI Tool
AEX-AR9590-NX, Compex WLE900 VX, Doodle labs NO-DB-3U

Location as a Service is now a commonplace



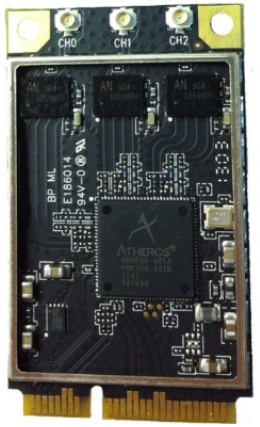
NEXMON CSI Tool
ASUS RT-AC86U

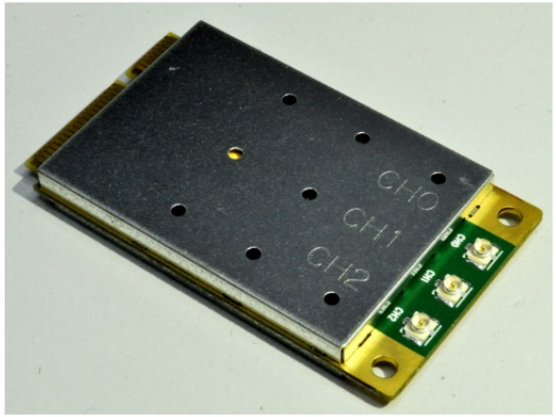
ON Semiconductor

Qualcomm

Quantenna

Intel-PicoScenes
Intel AX200, IWL 5300, QCA9300, SDRs





Atheros CSI Tool
AEX-AR9590-NX, Compex WLE900 VX, Doodle labs NO-DB-3U

Location as a Service is now a commonplace

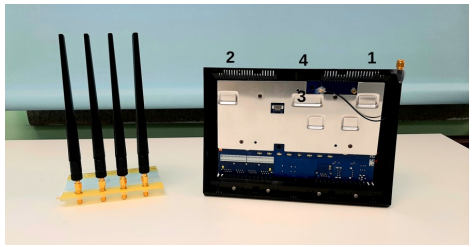
cisco DNA Spaces

JUNIPER NETWORKS

ON Semiconductor

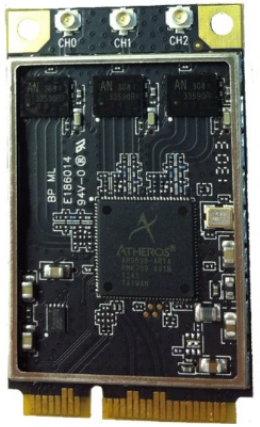
Qualcomm

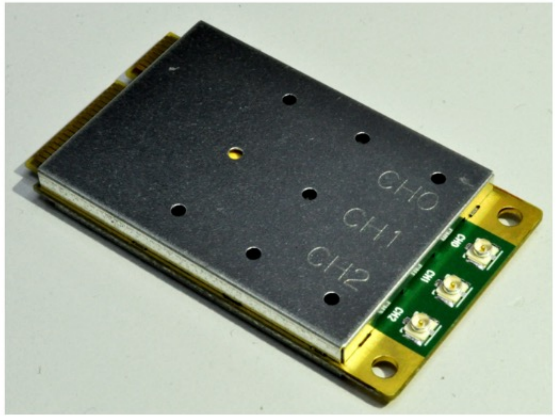
Quantenna



NEXMON CSI Tool
ASUS RT-AC86U

Intel-PicoScenes
Intel AX200, IWL 5300, QCA9300, SDRs





Atheros CSI Tool
AEX-AR9590-NX, Compex WLE900 VX, Doodle labs NO-DB-3U

Your Device Location is no longer safe

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Enforcement | Policy | Advice and Guidance | News and Events | About the FTC

Home / News and Events / News / Press Releases

For Release

Retail Tracking Firm Settles FTC Charges it Misled Consumers About Opt Out Choices

Company Falsely Promised an In-Store Opt Out, Agency Alleges

April 23, 2015

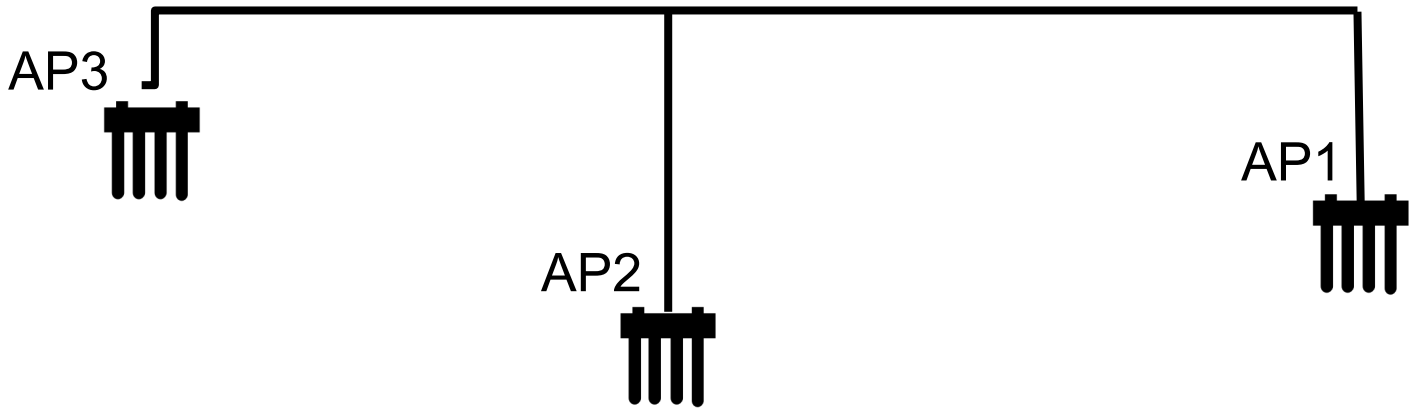
Tags: Consumer Protection | Bureau of Consumer Protection | Retail | Technology | Privacy and Security | Consumer Privacy | FinTech

Related Cases

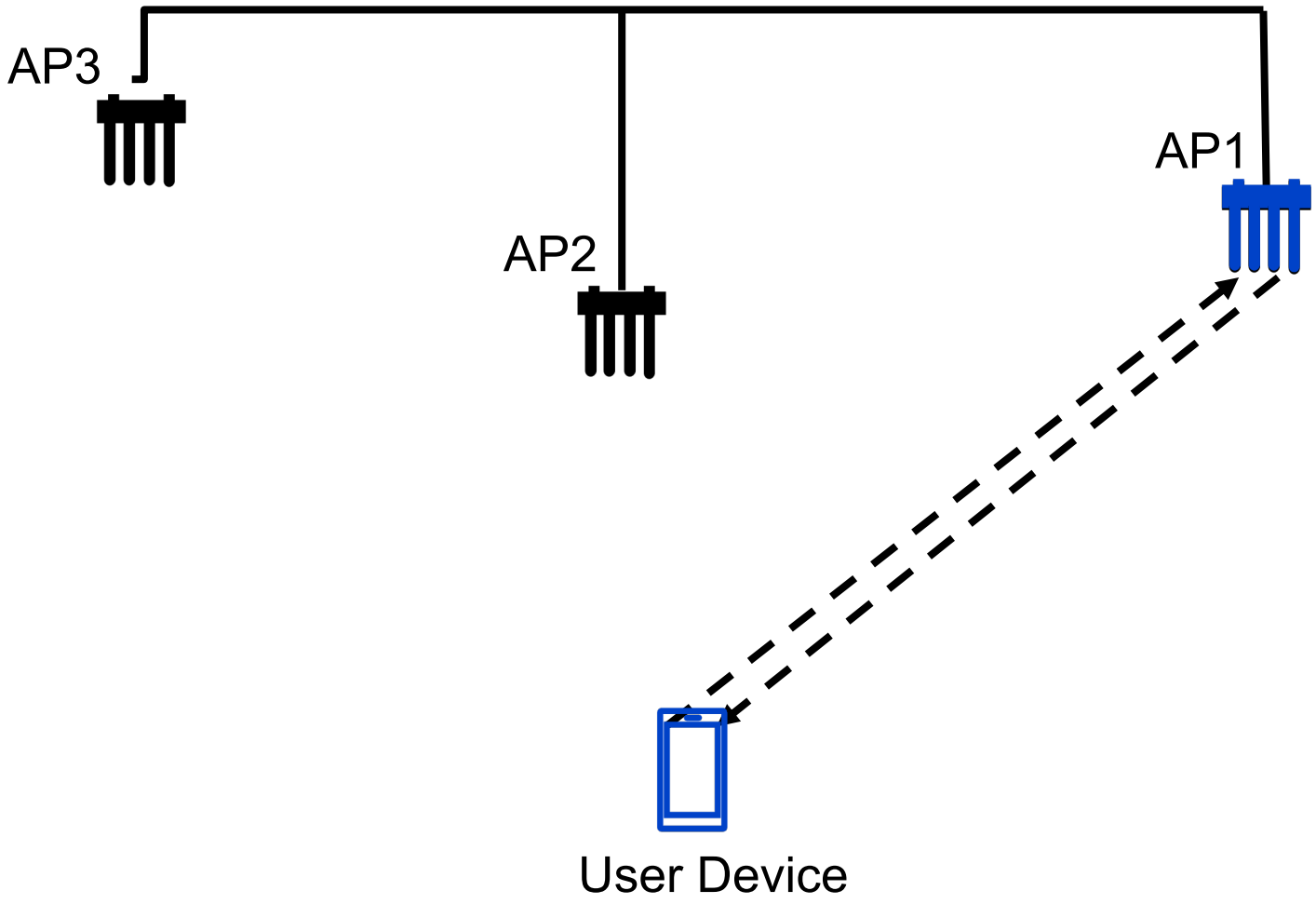
Nomi Technologies, Inc., In the Matter

Attack Model – Enterprise Network

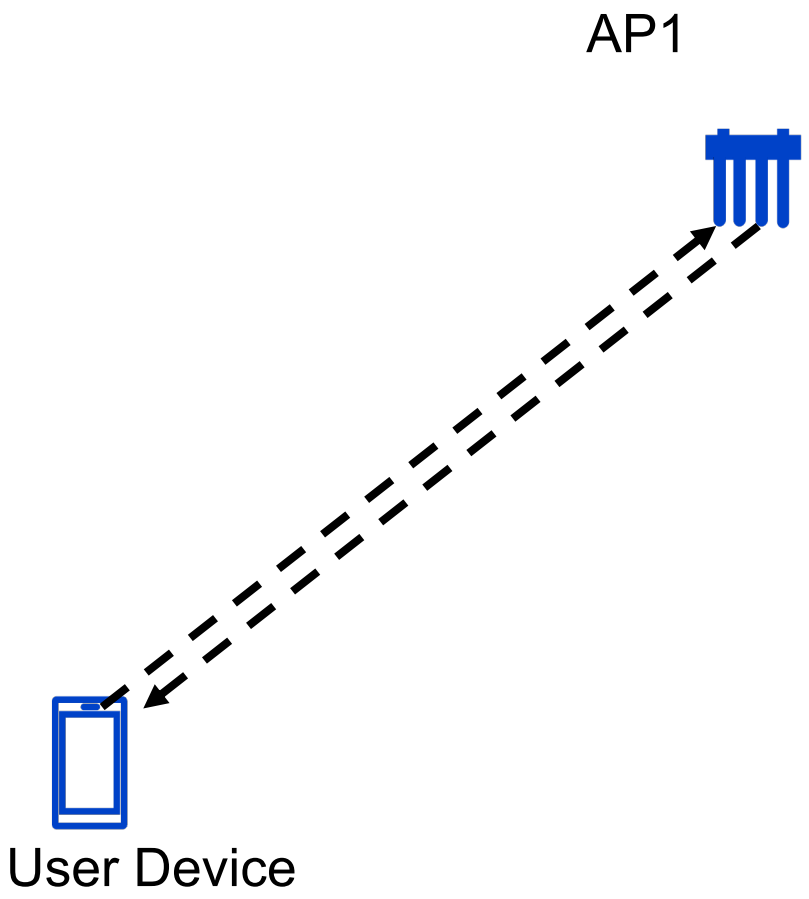
Attack Model – Enterprise Network



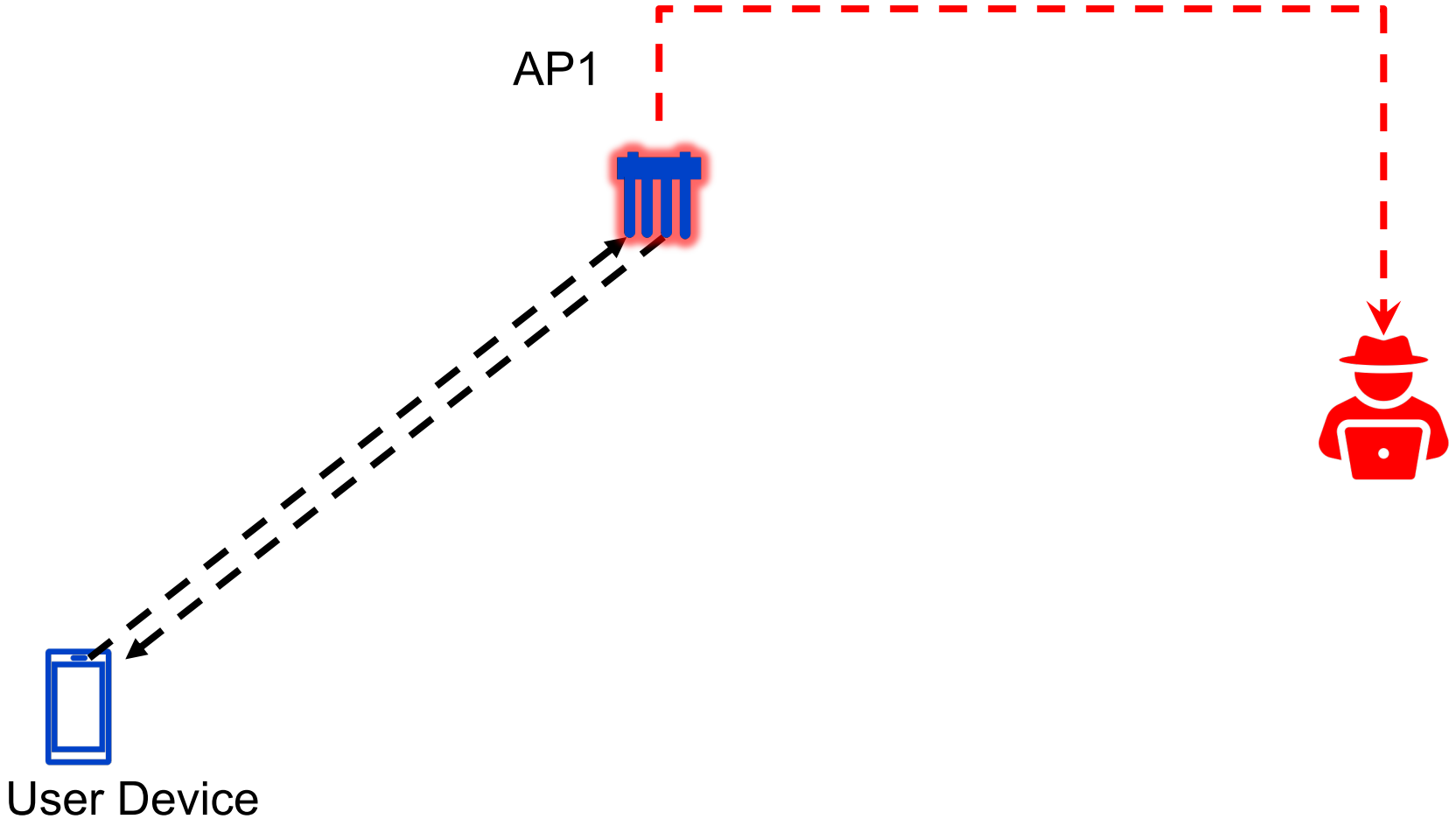
Attack Model – Enterprise Network



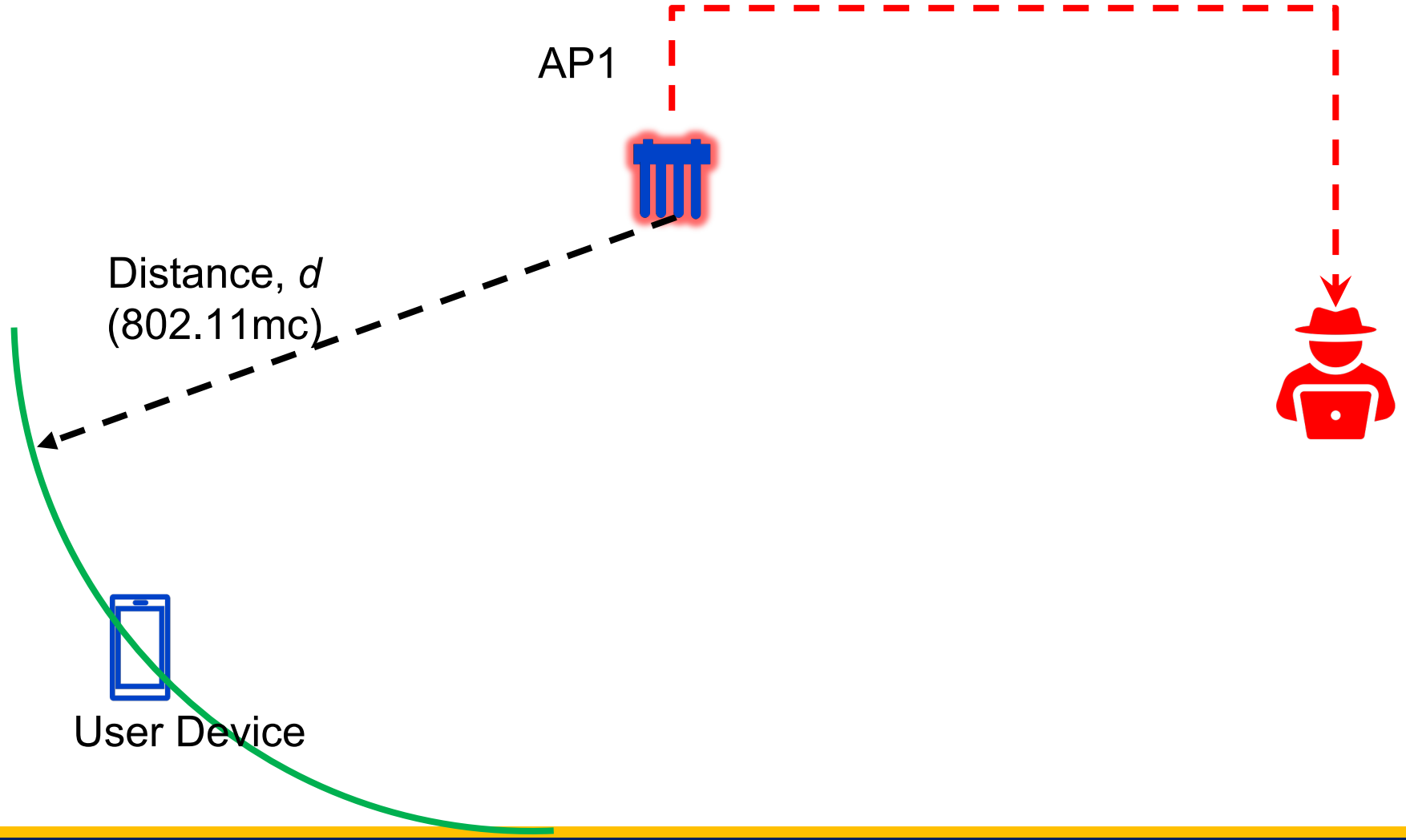
Attack Model – Single AP



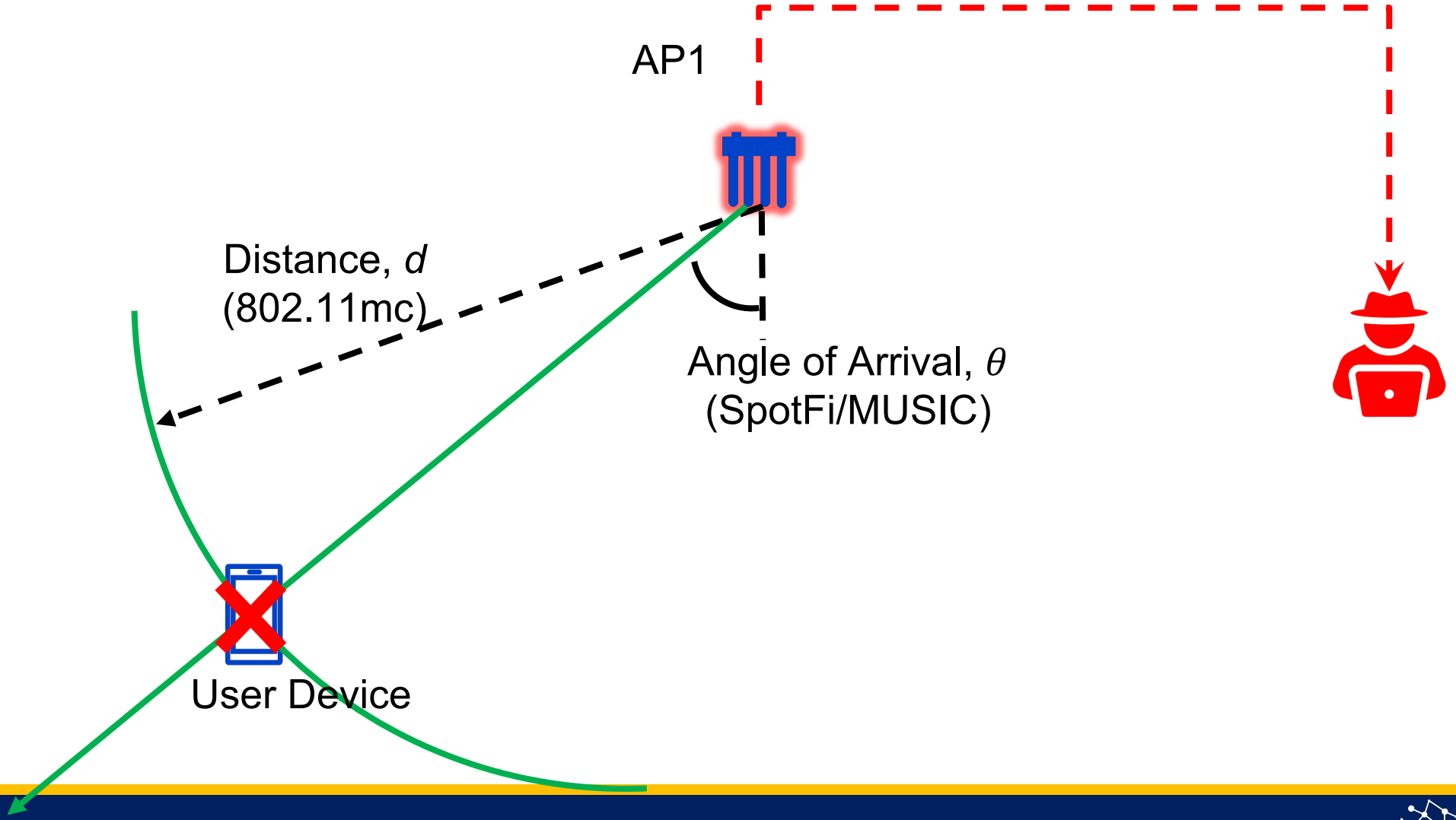
Attack Model – Single AP



Attack Model – Single AP

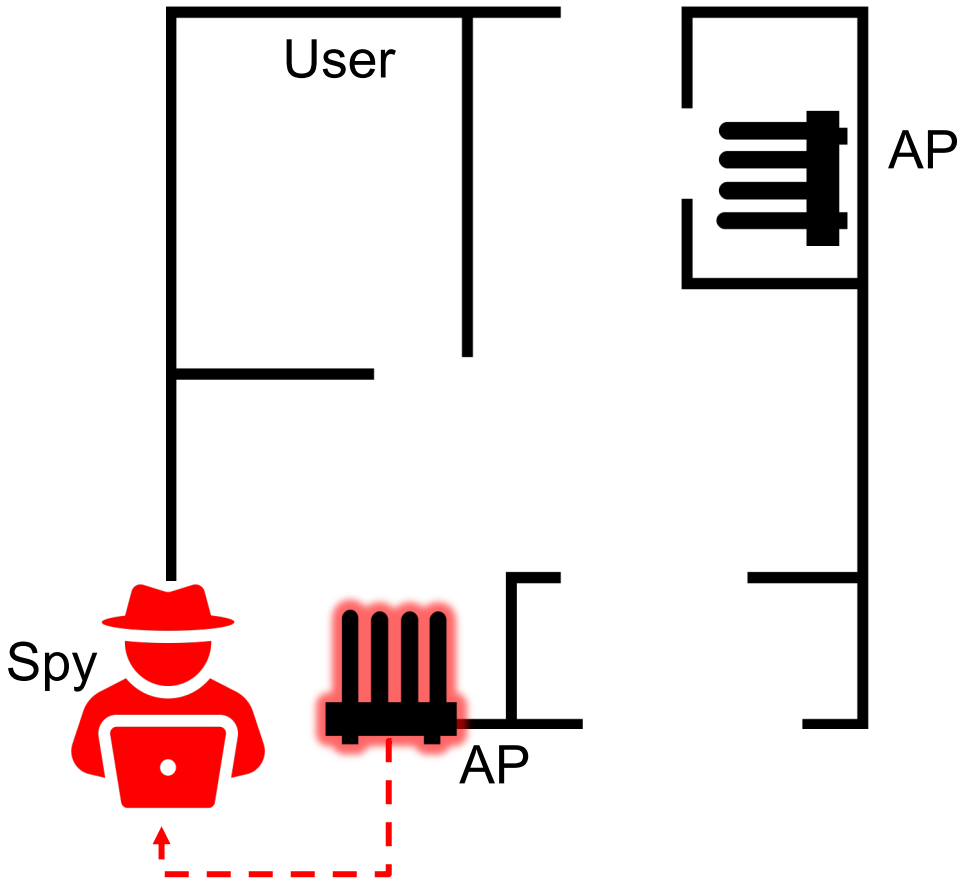


Attack Model – Single AP

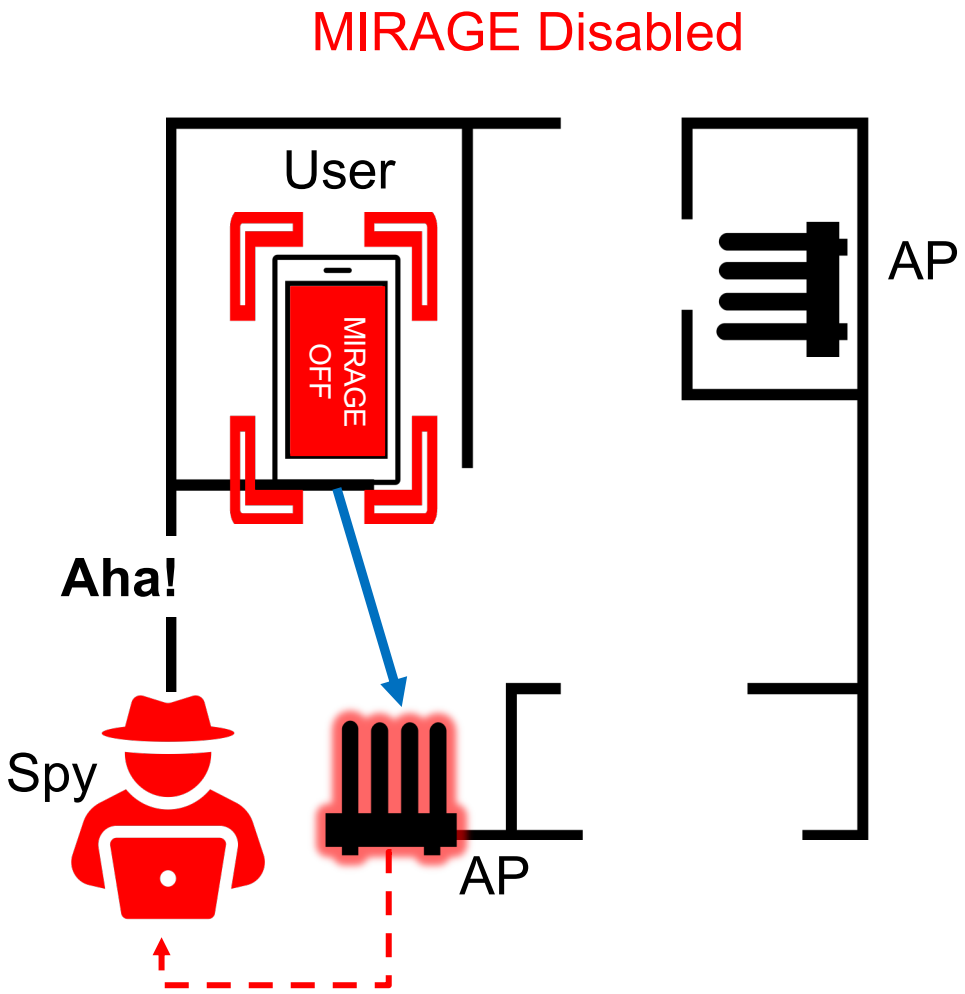


MIRAGE – Enabling location privacy

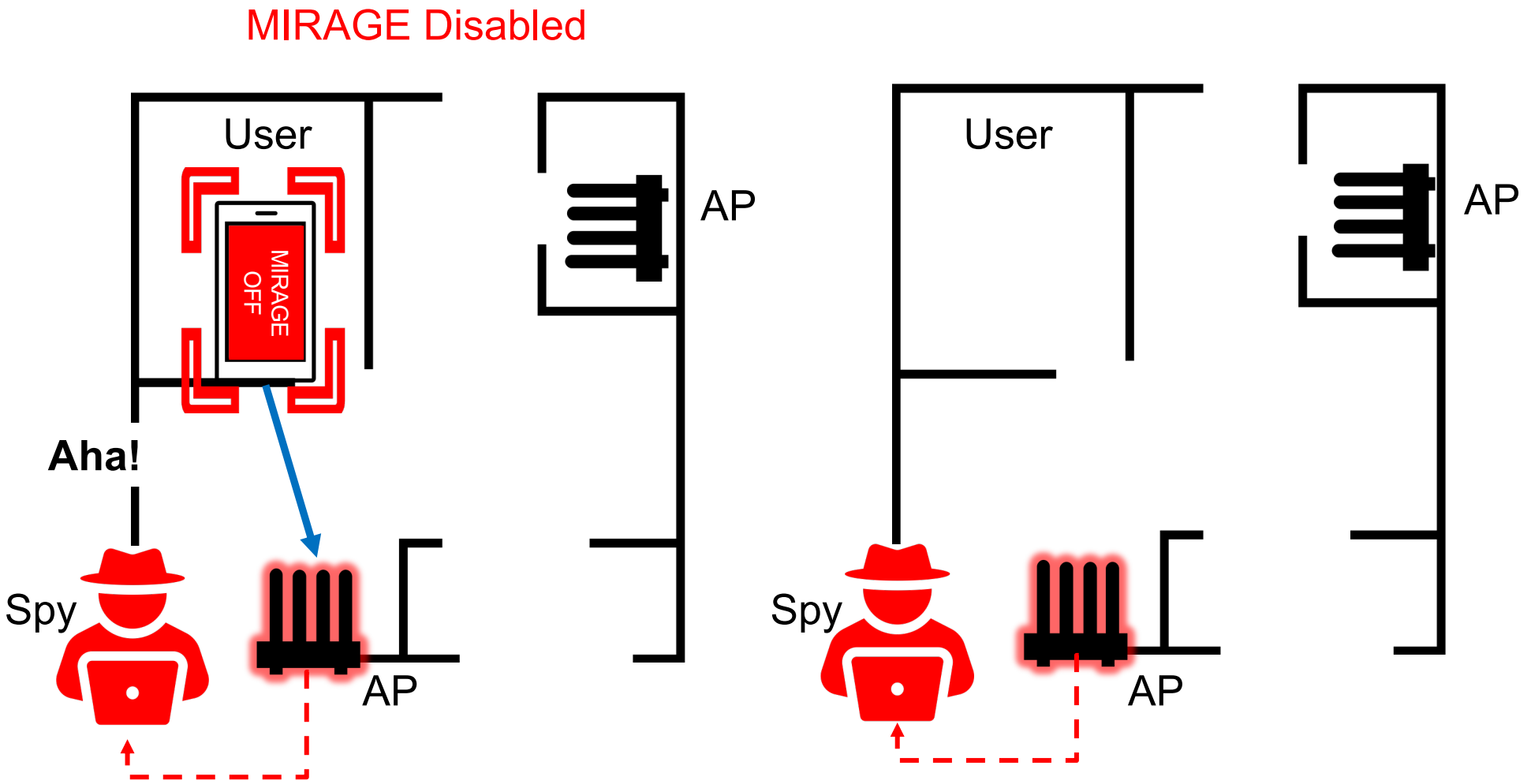
MIRAGE – Enabling location privacy



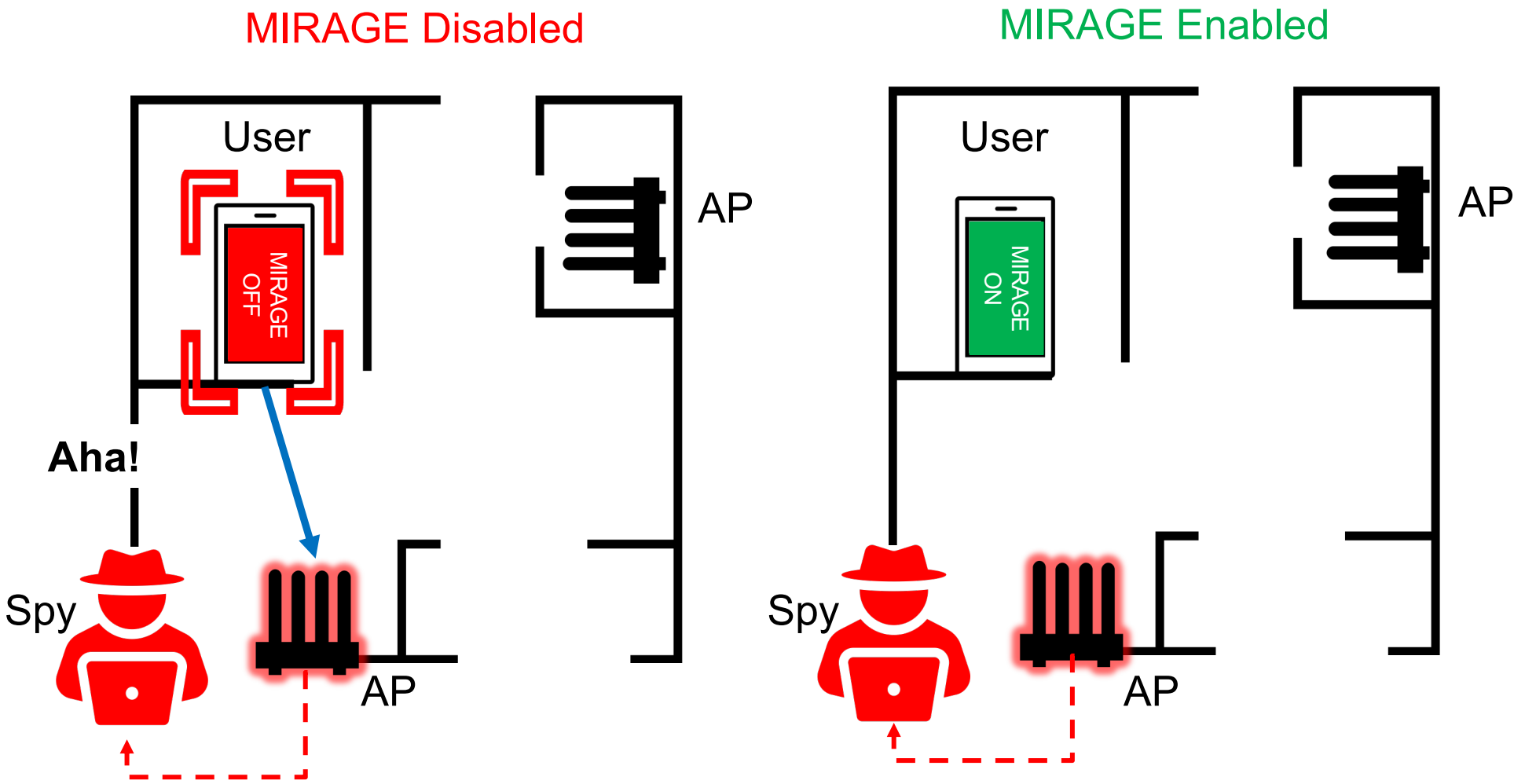
MIRAGE – Enabling location privacy



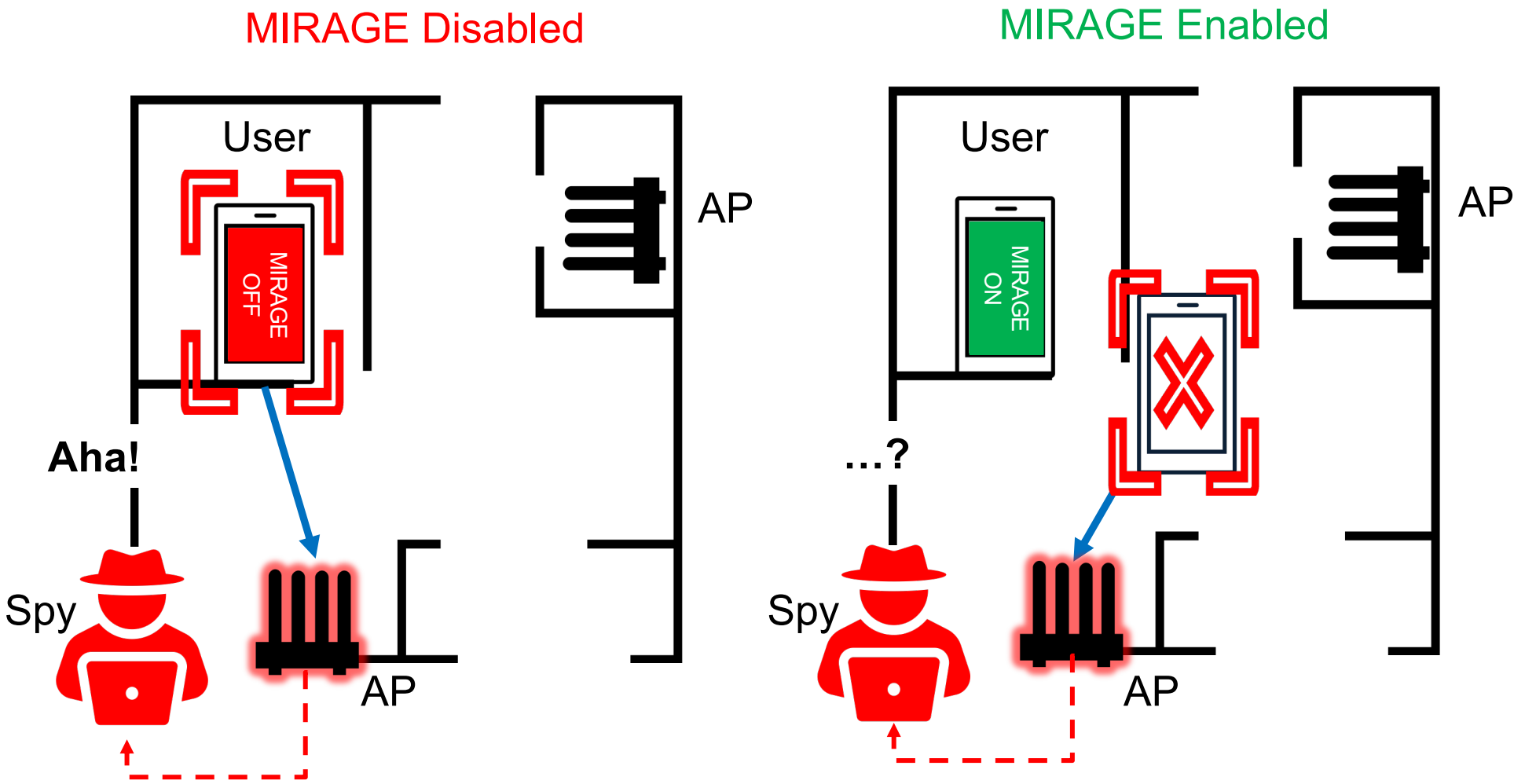
MIRAGE – Enabling location privacy



MIRAGE – Enabling location privacy



MIRAGE – Enabling location privacy



Requirements for MIRAGE's implementation

Requirements for MIRAGE's implementation

(R.1) Robust location obfuscation.

Requirements for MIRAGE's implementation

(R.1) Robust location obfuscation.

(R.2) Does not compromise the communication link.

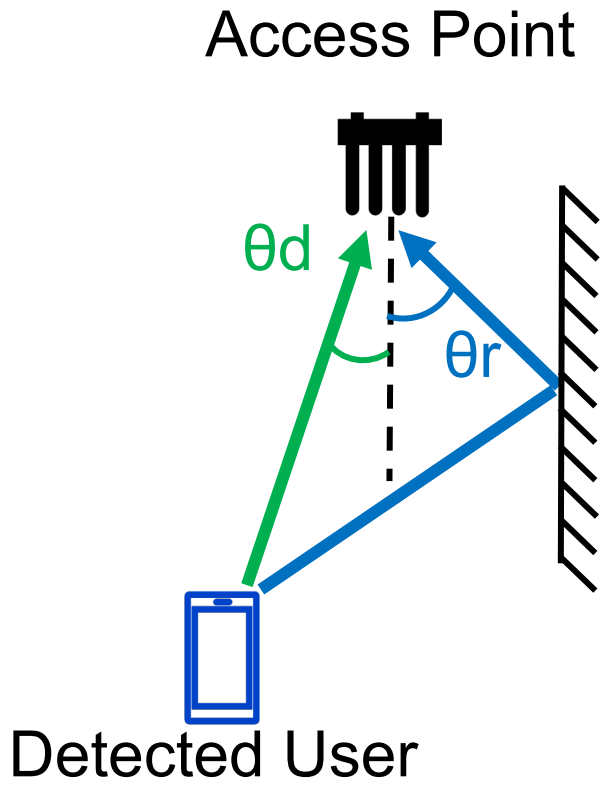
Requirements for MIRAGE's implementation

(R.1) Robust location obfuscation.

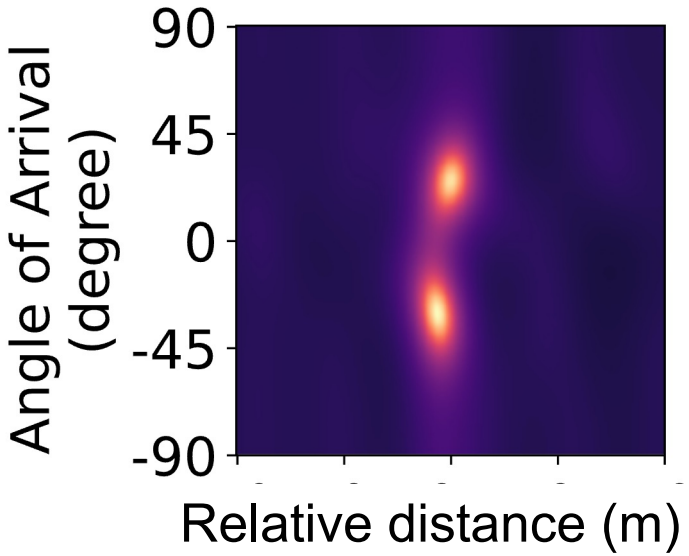
(R.2) Does not compromise the communication link.

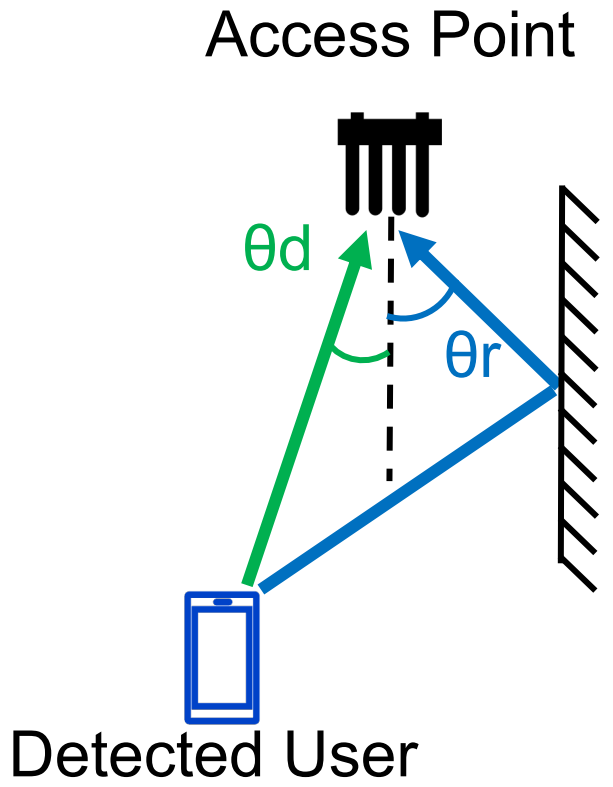
(R.3) Attacker cannot decode location with the knowledge of defense model.

Direct Path – Least Traveled Path

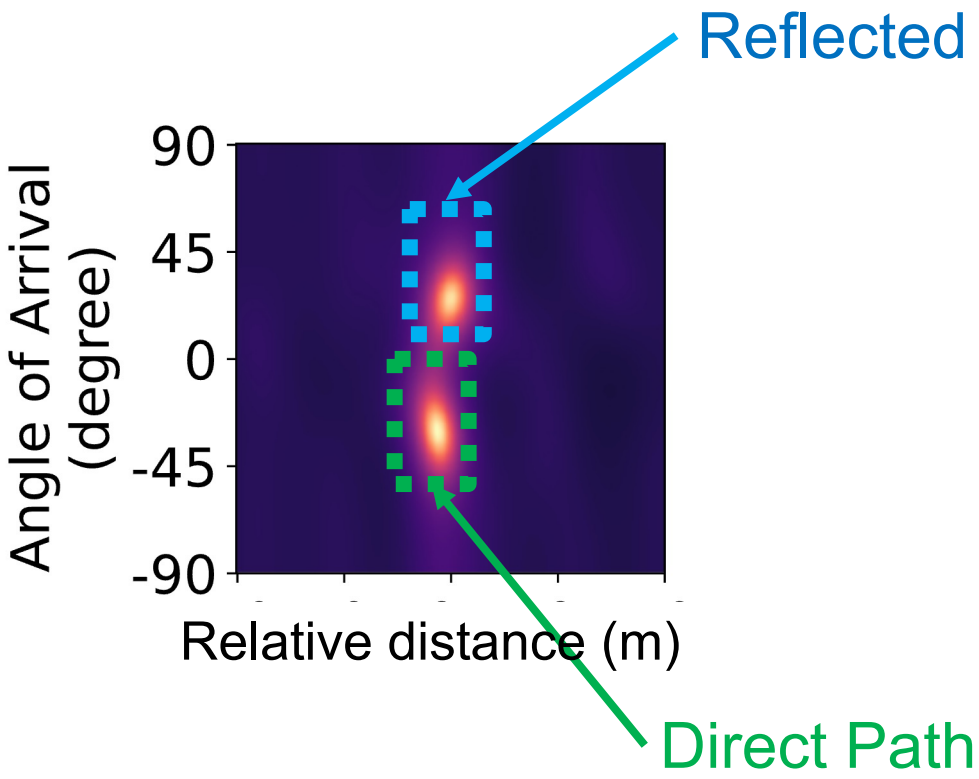


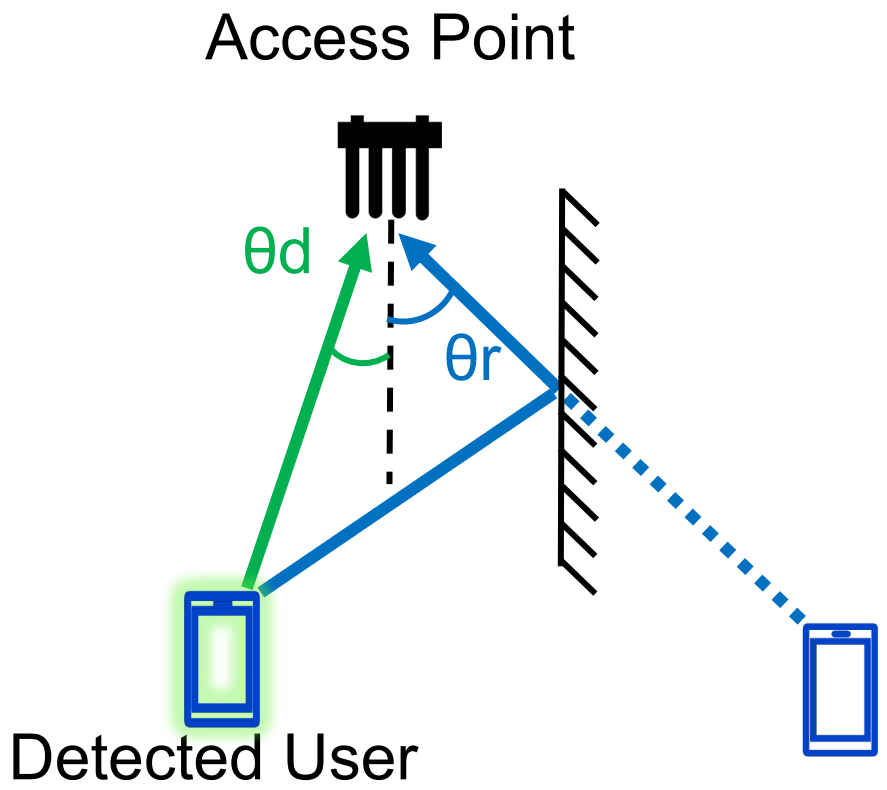
Direct Path – Least Traveled Path



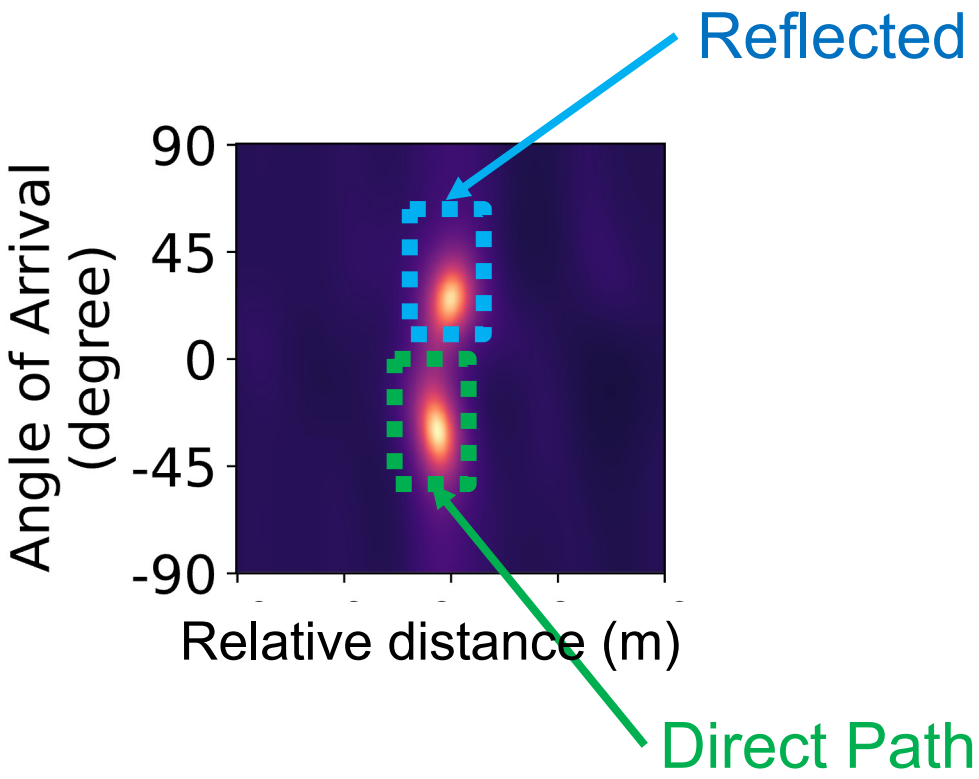


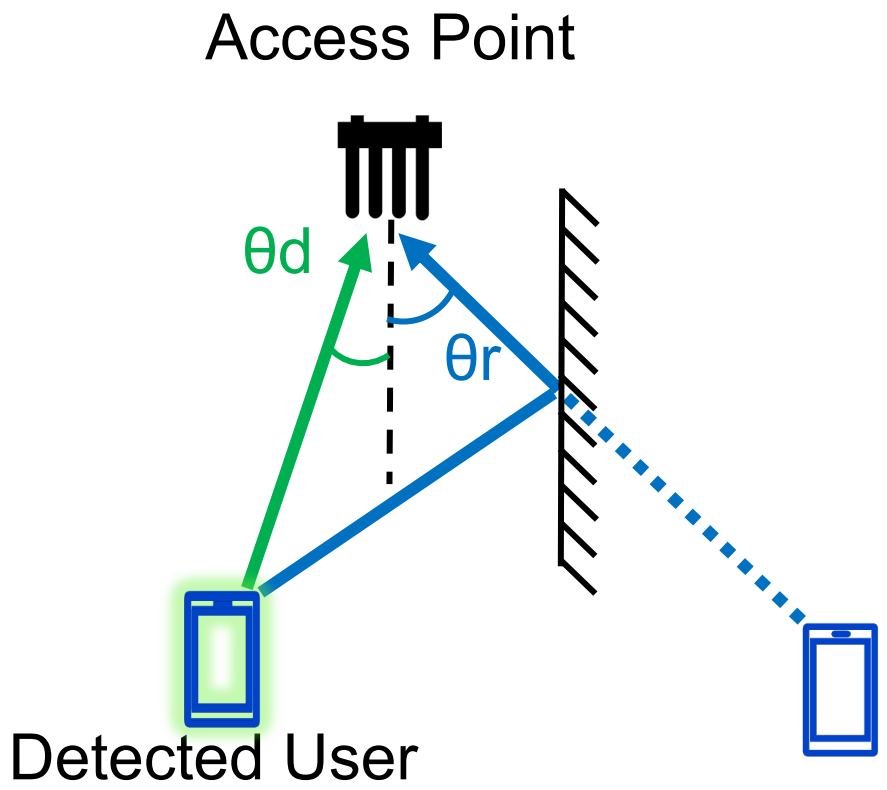
Direct Path – Least Traveled Path





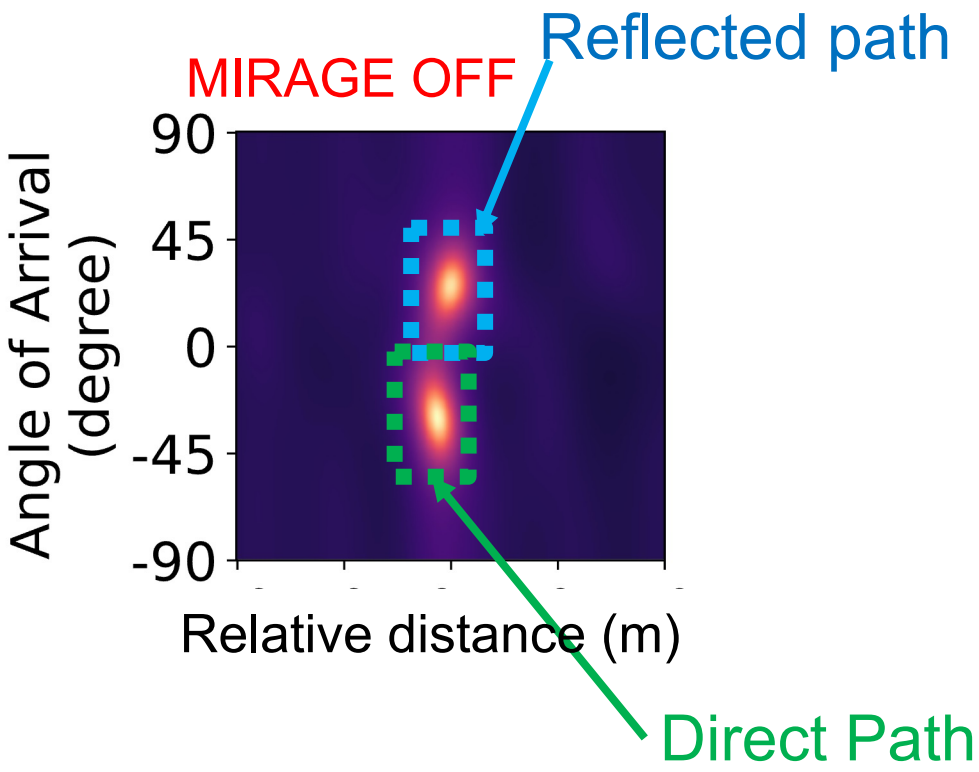
Direct Path – Least Traveled Path

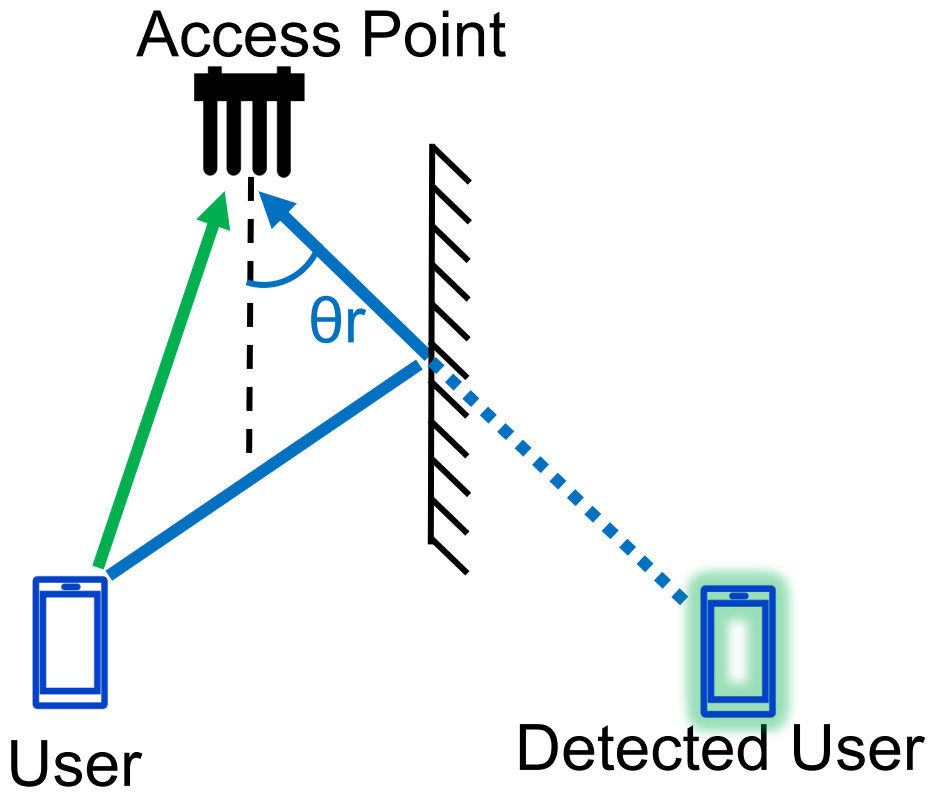




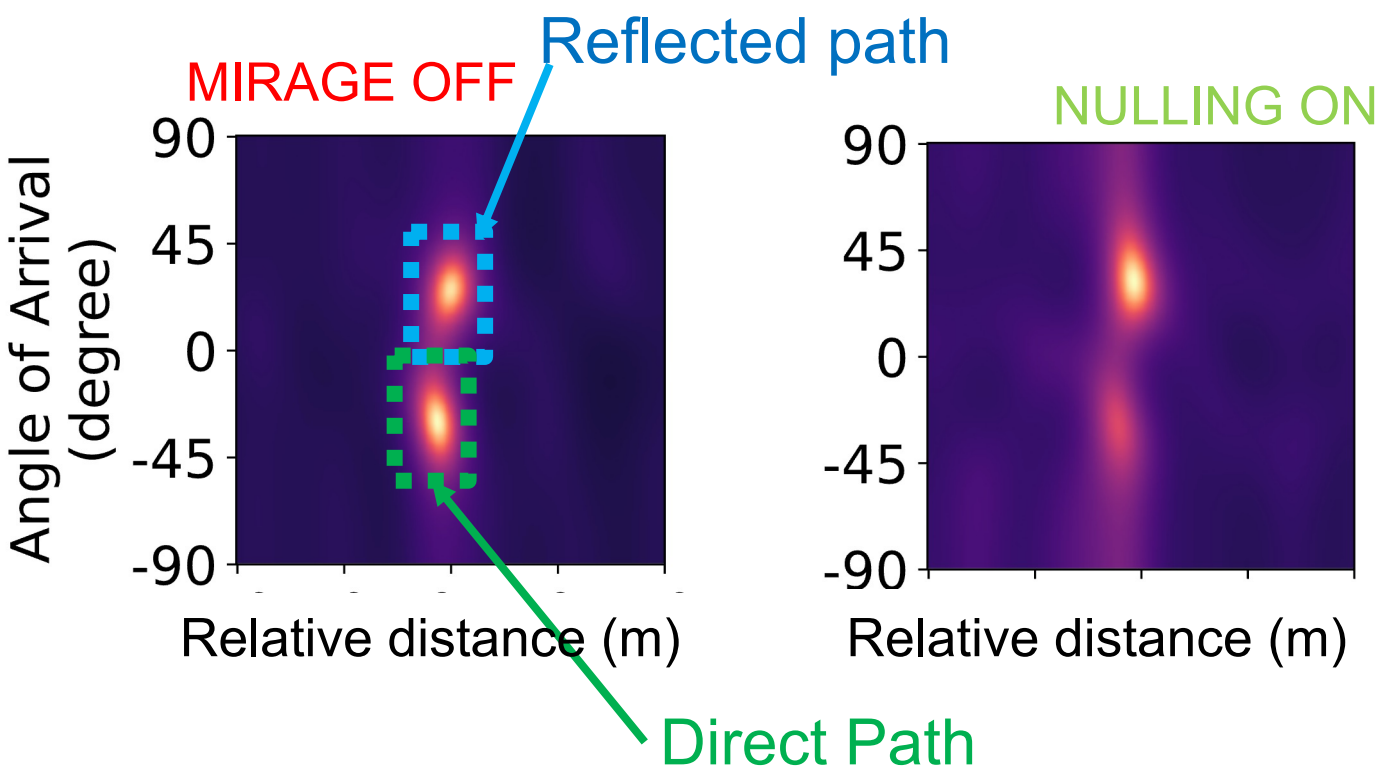
How can we ensure Attacker does not know Direct Path?

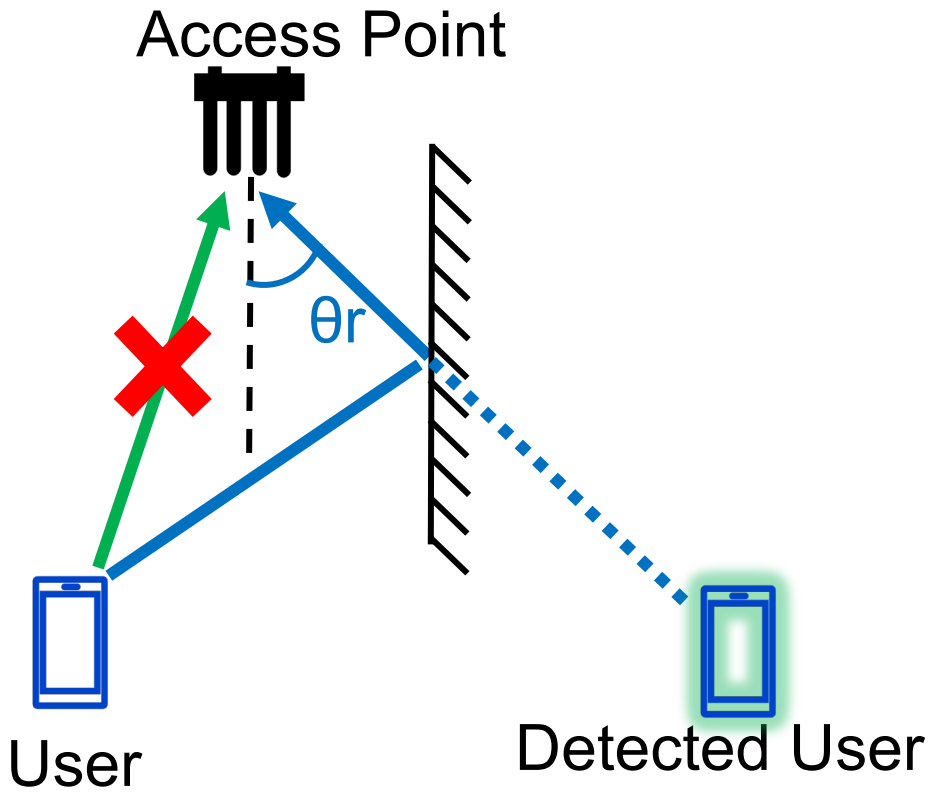
Remove the Direct path



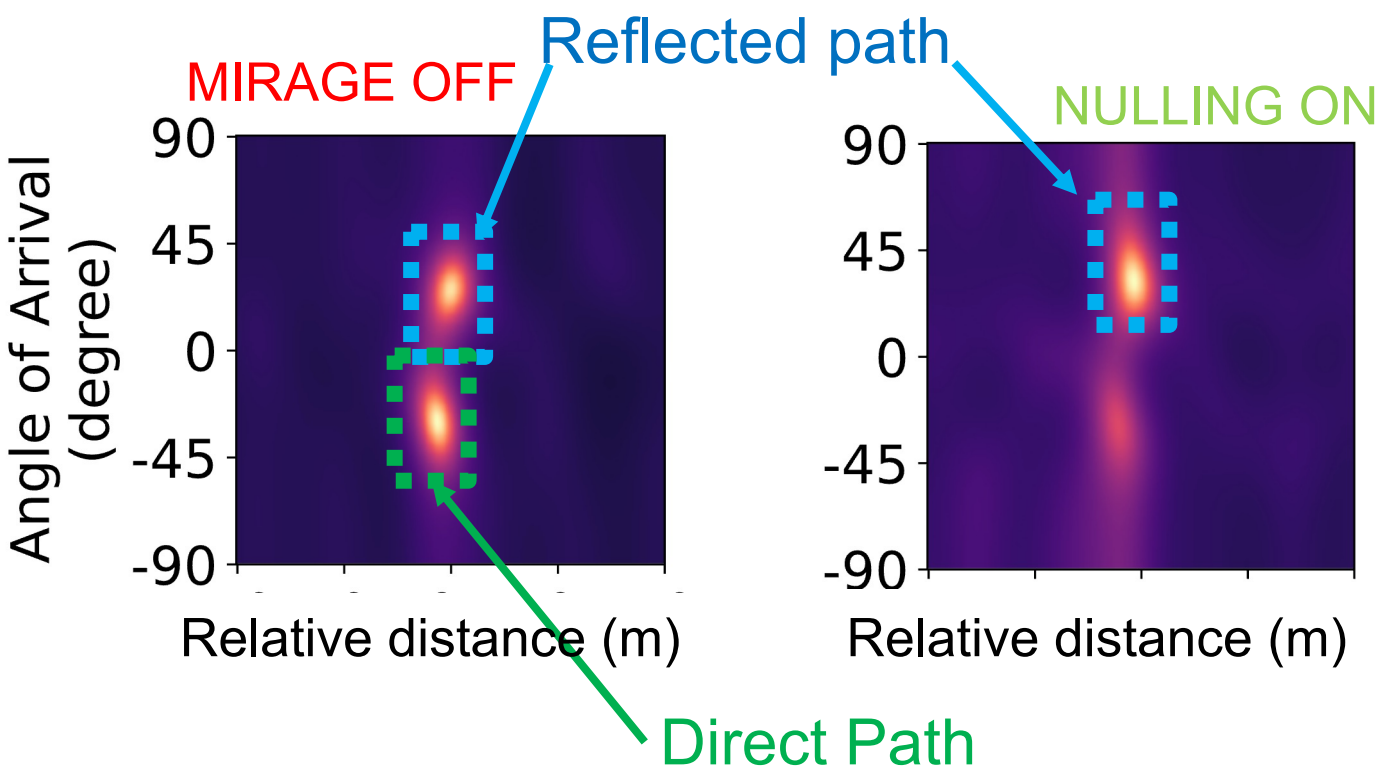


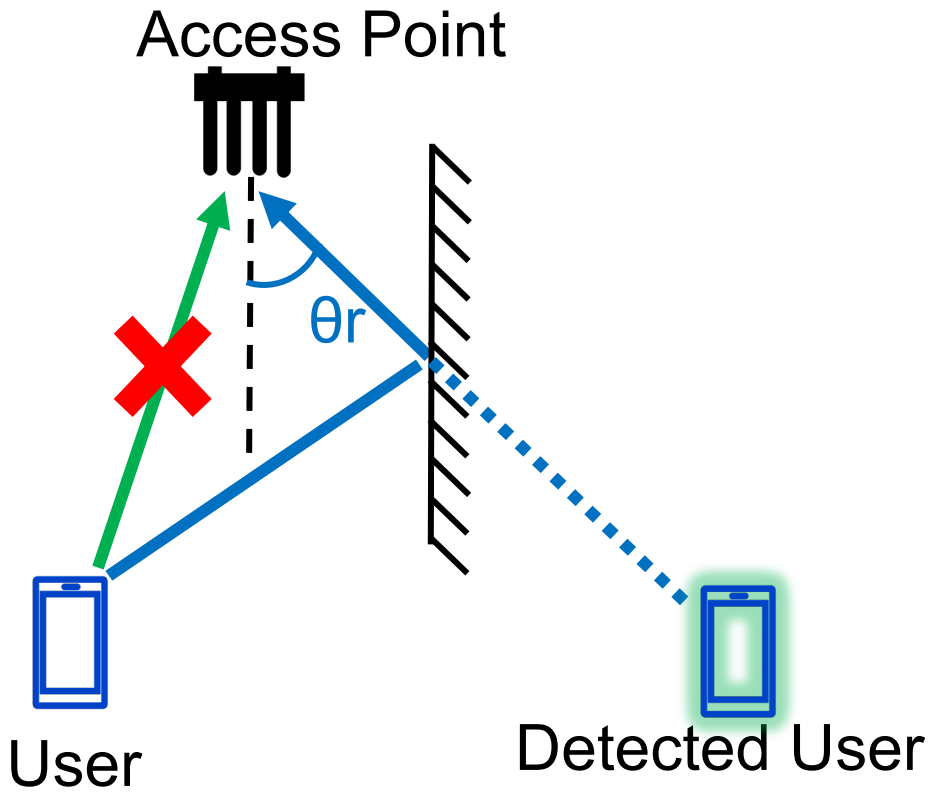
Remove the Direct path





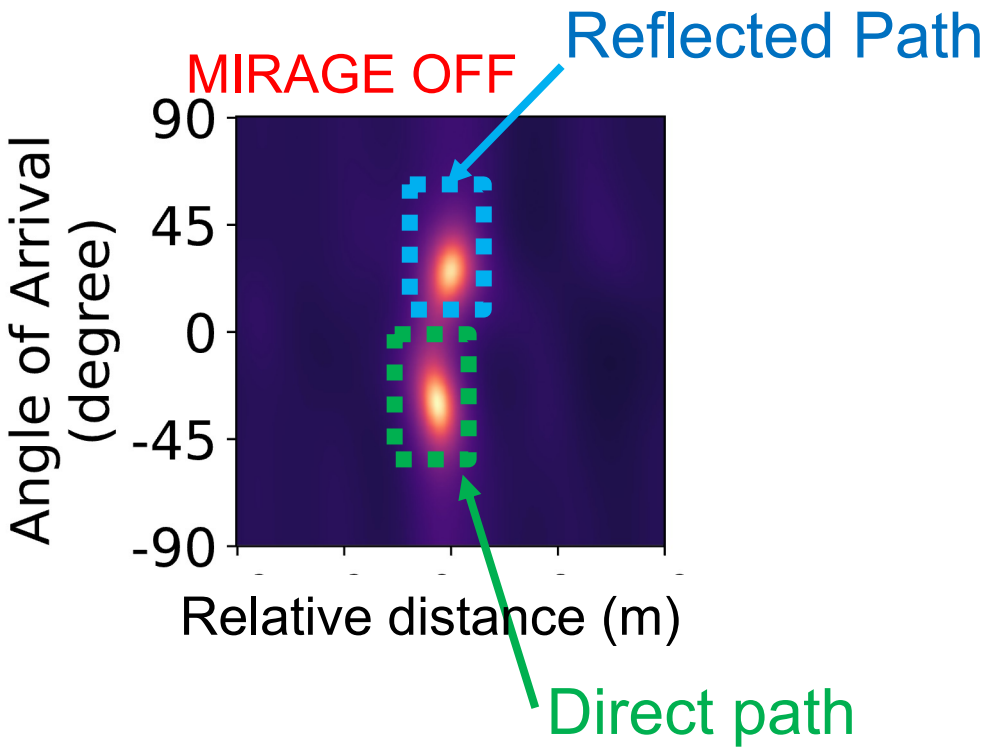
Remove the Direct path

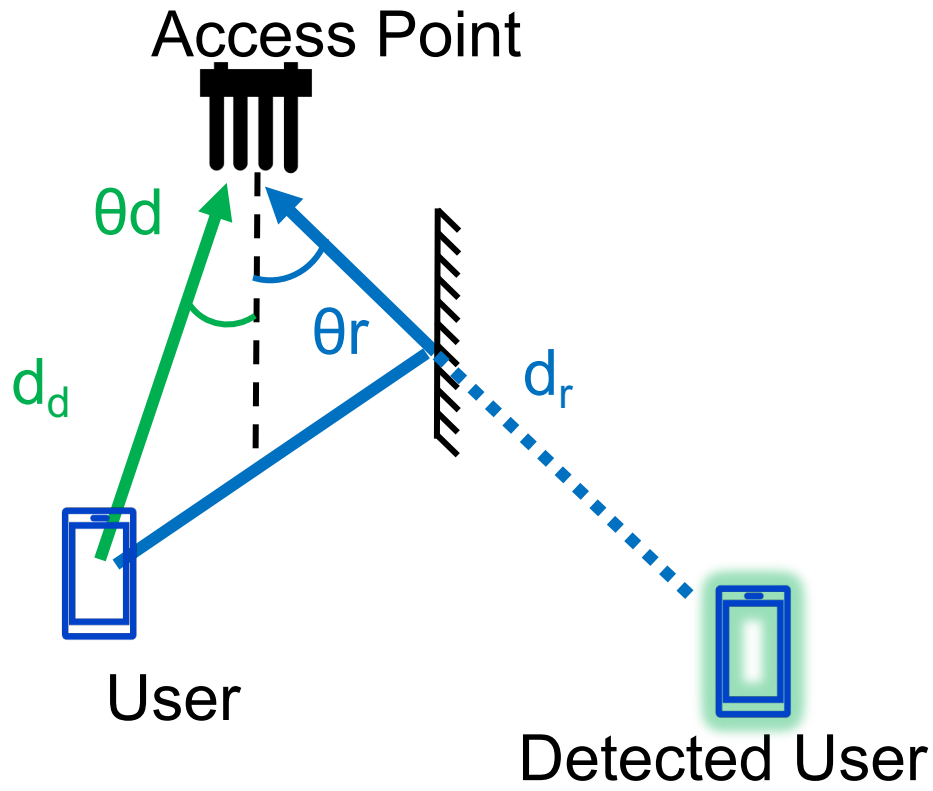




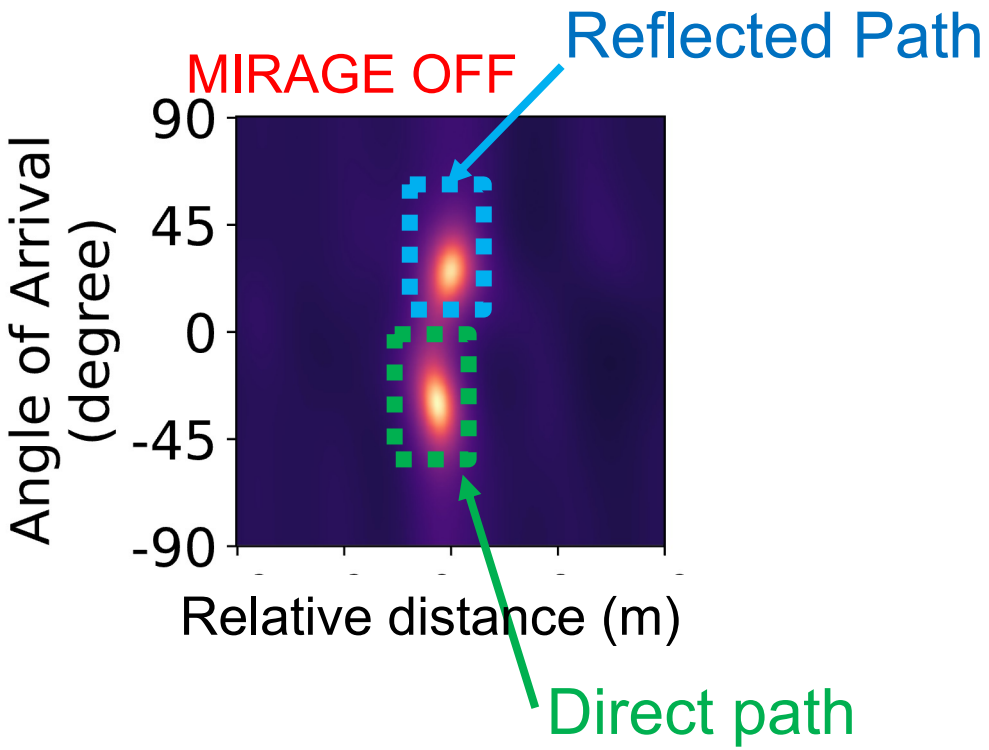
Nulling – Reduced SNR

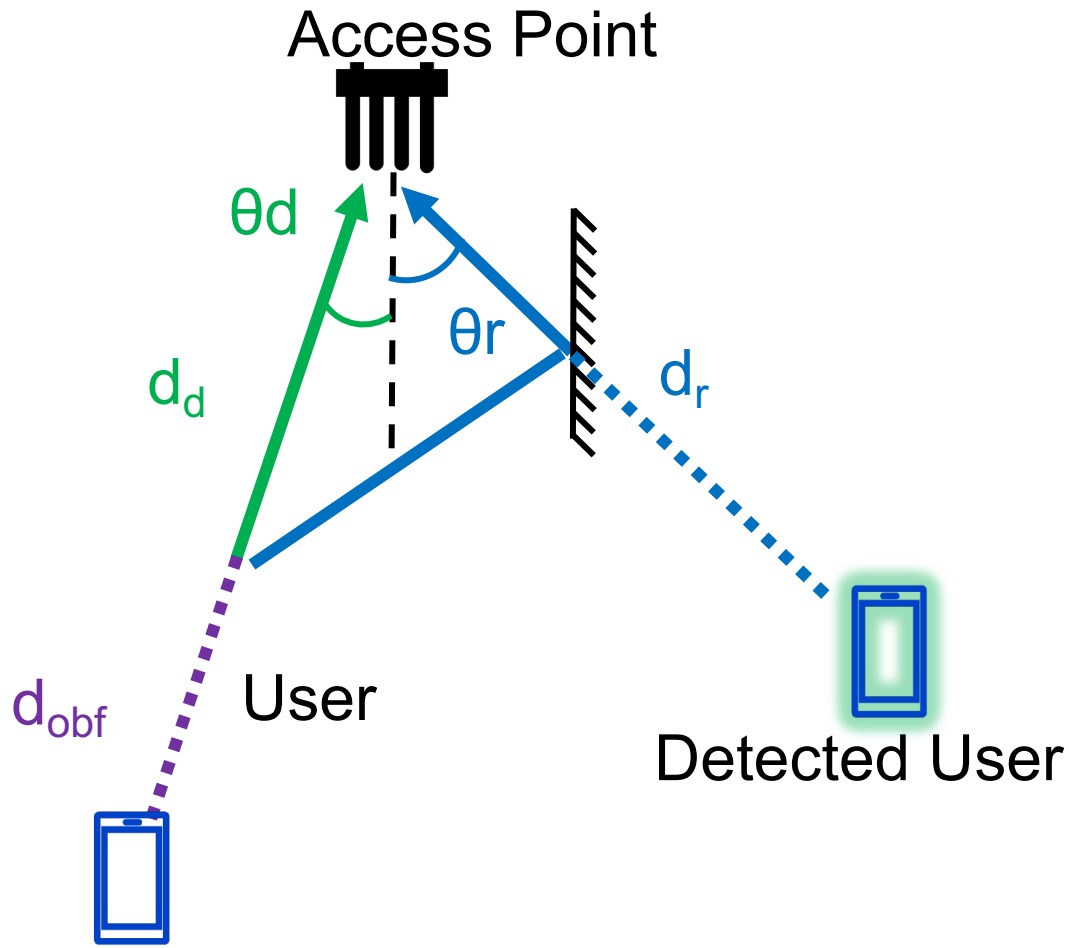
Obfuscate the Direct Path



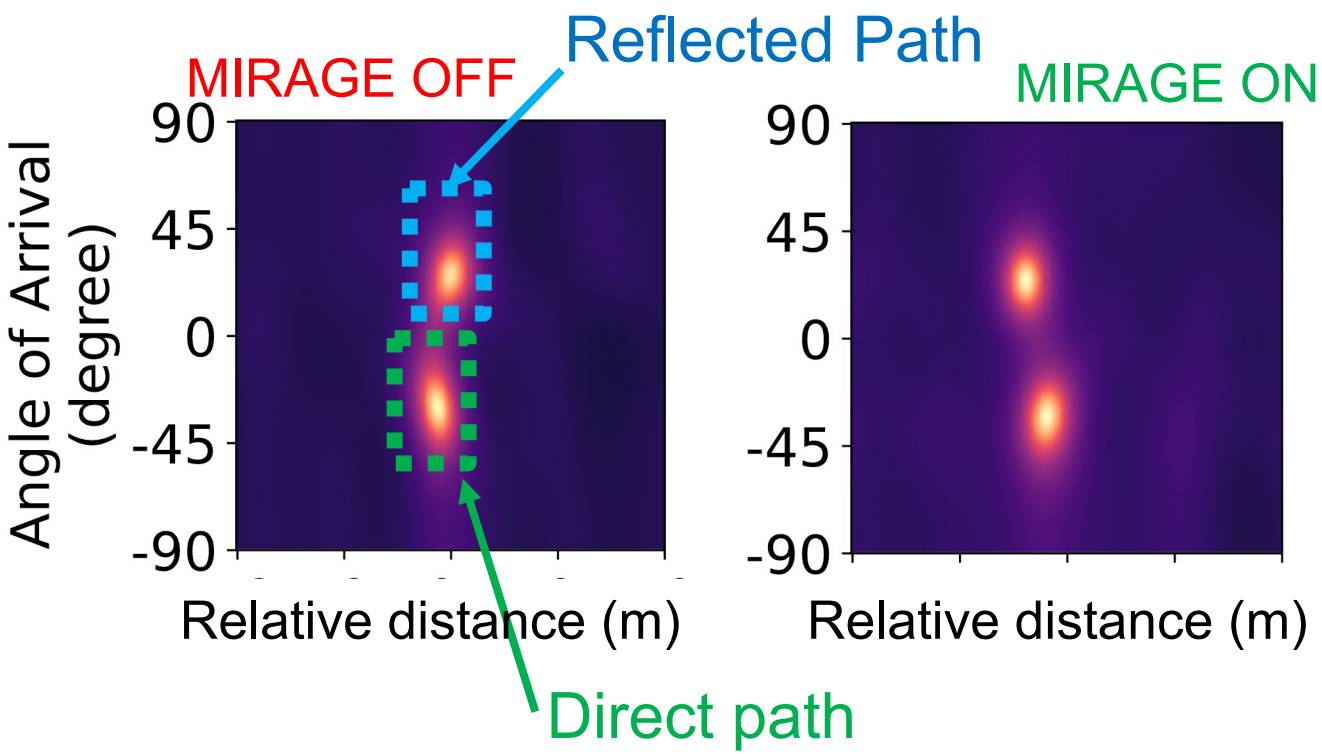


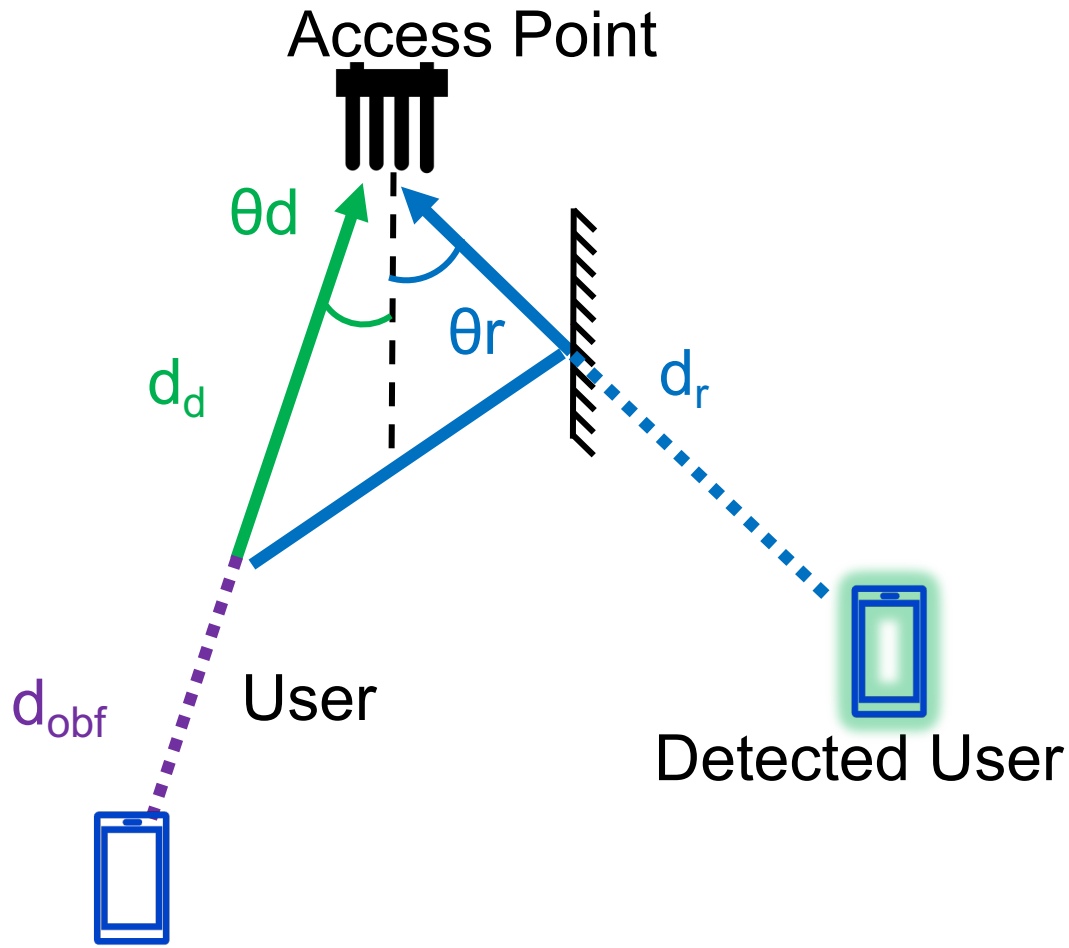
Obfuscate the Direct Path



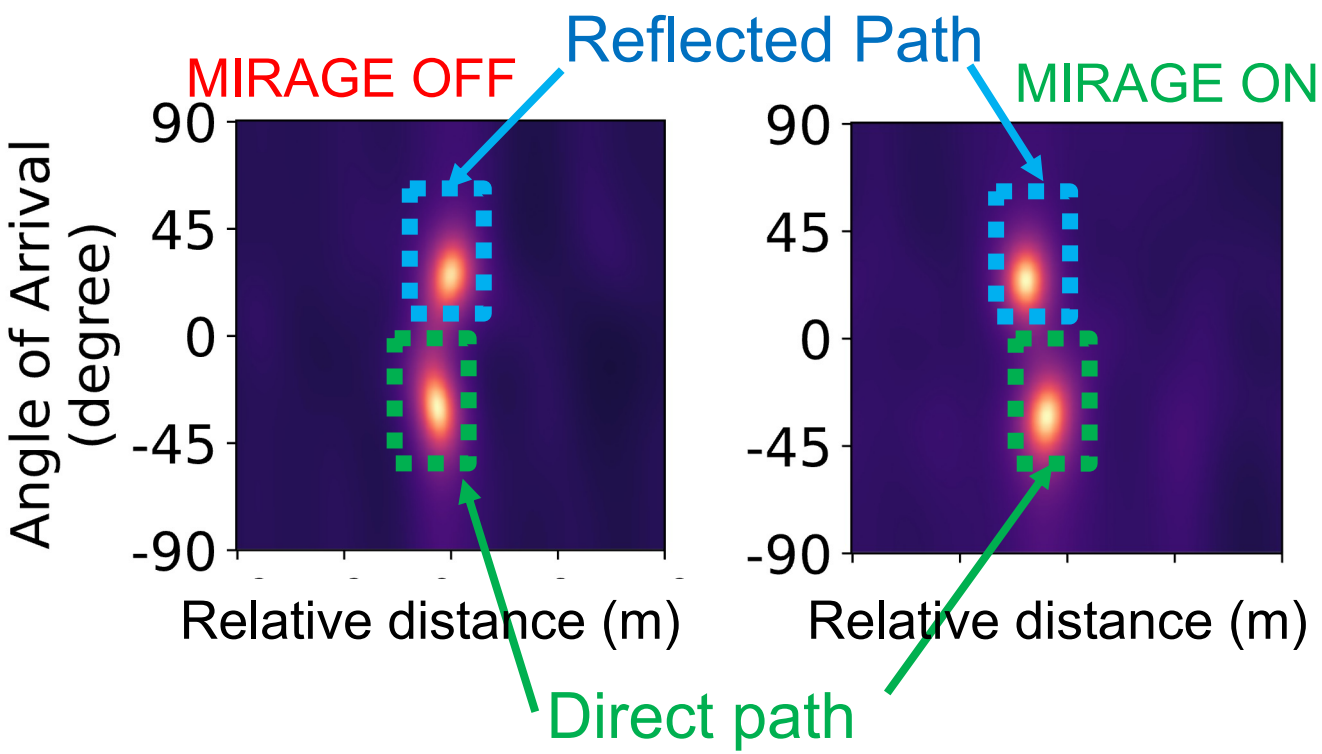


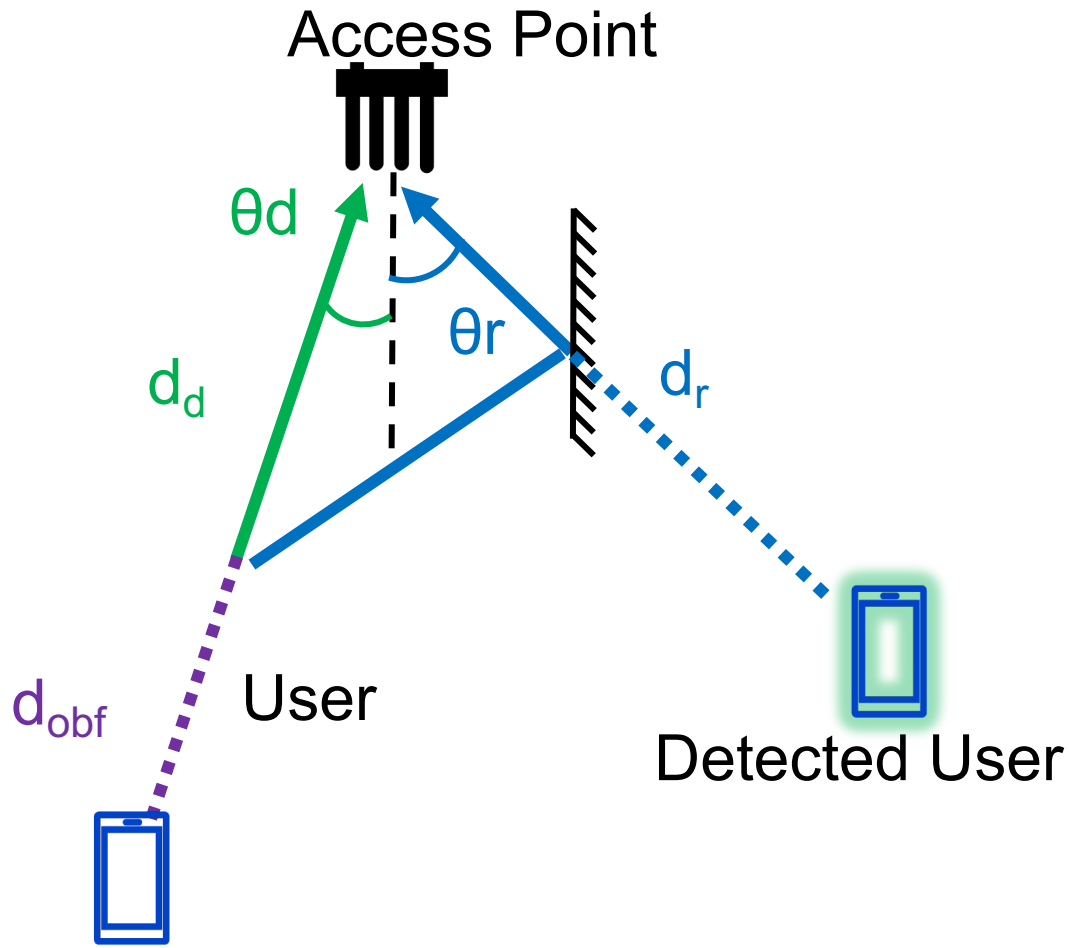
Obfuscate the Direct Path



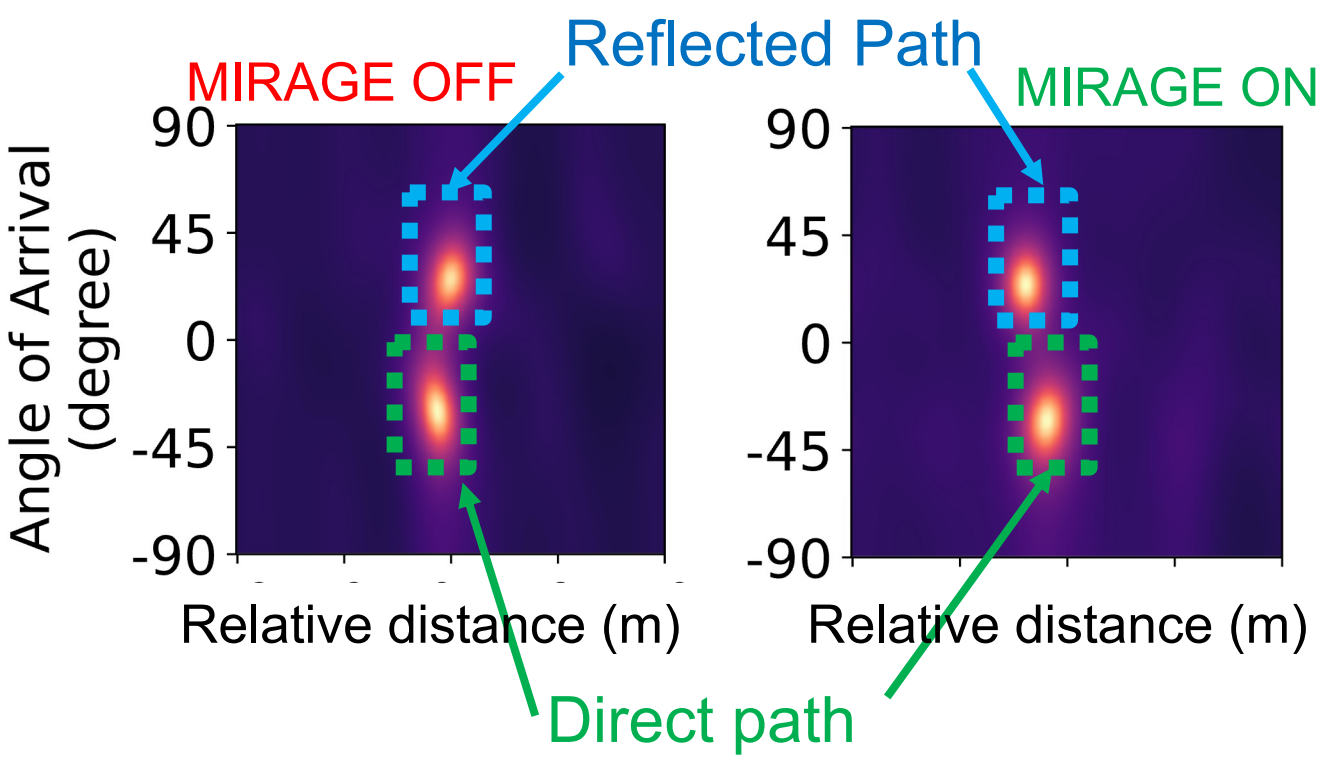


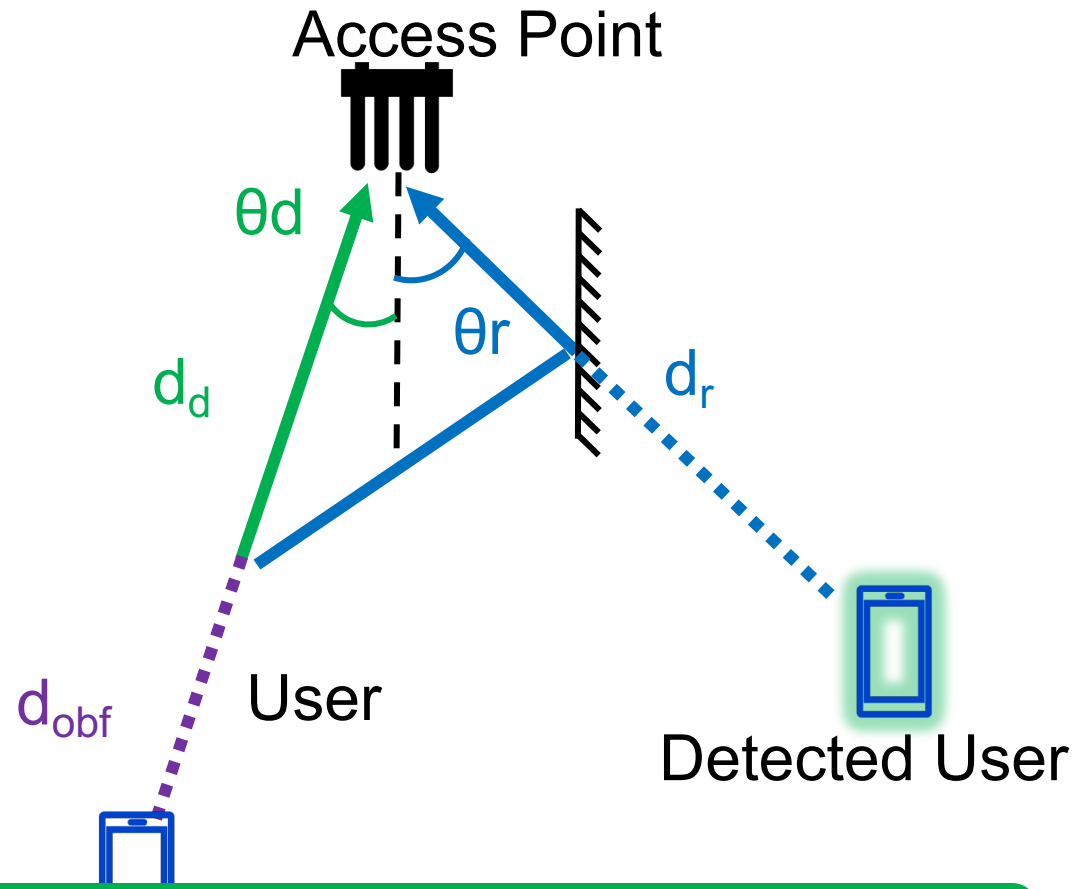
Obfuscate the Direct Path





Obfuscate the Direct Path

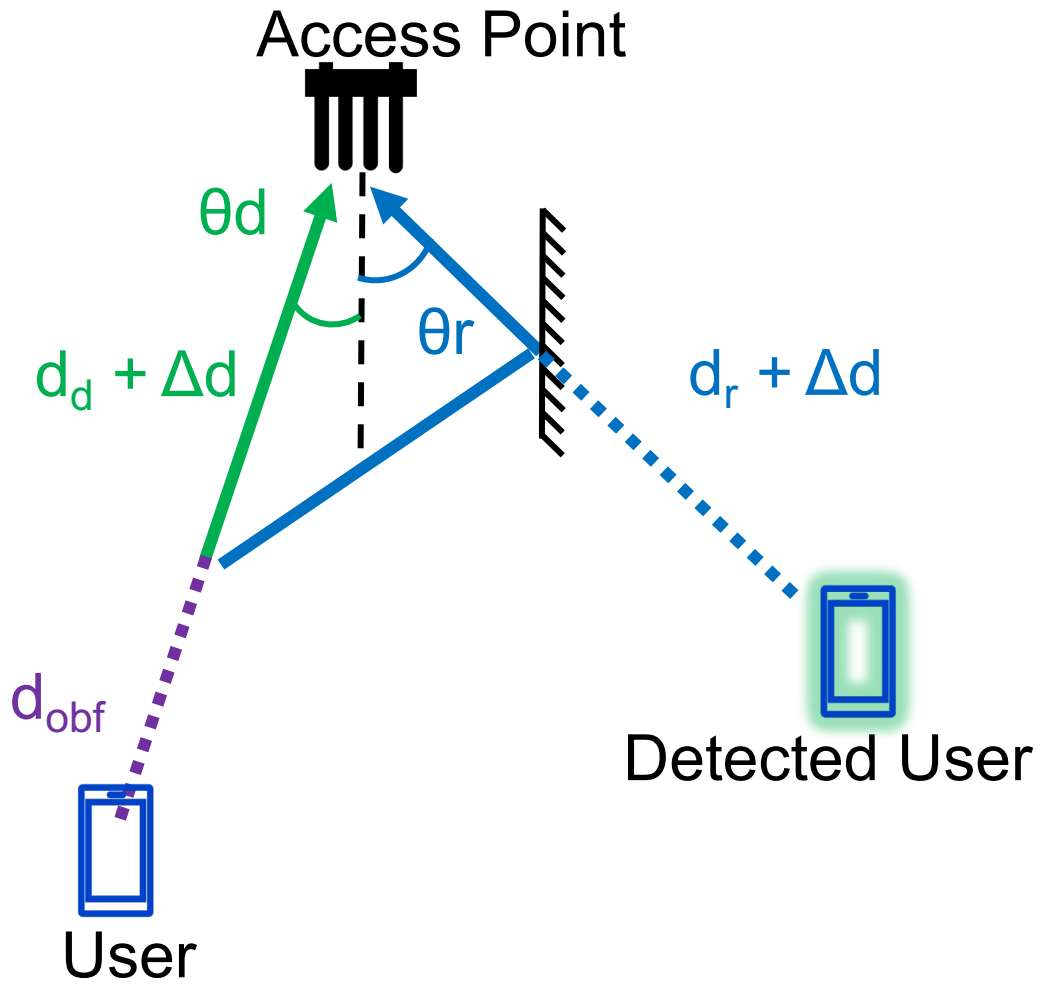




Direct Path – No more least travelled path

Obfuscate the Direct Path

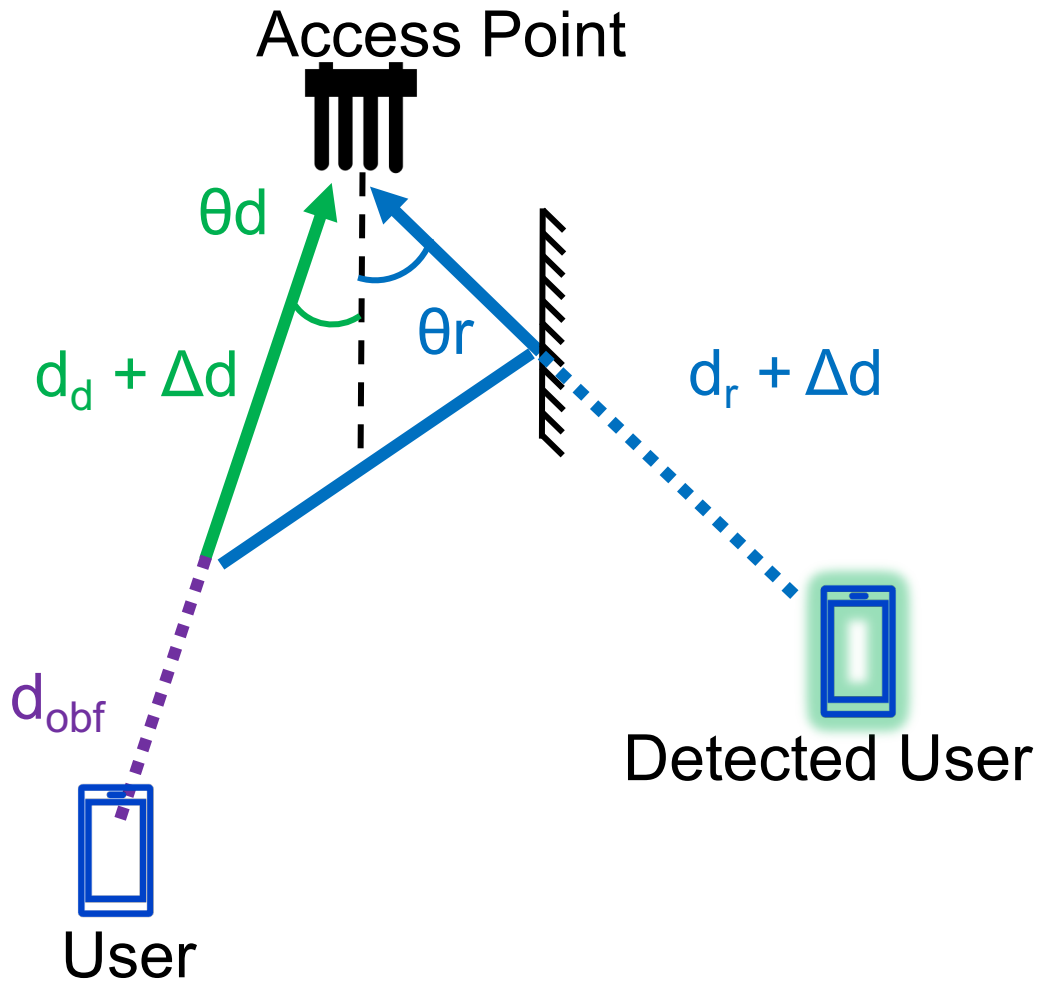
$$d_d + \Delta d < d_r + \Delta d$$



Obfuscate the Direct Path

$$d_d + \Delta d < d_r + \Delta d$$

$$d_d + \Delta d + d_{obf} > d_r + \Delta d$$

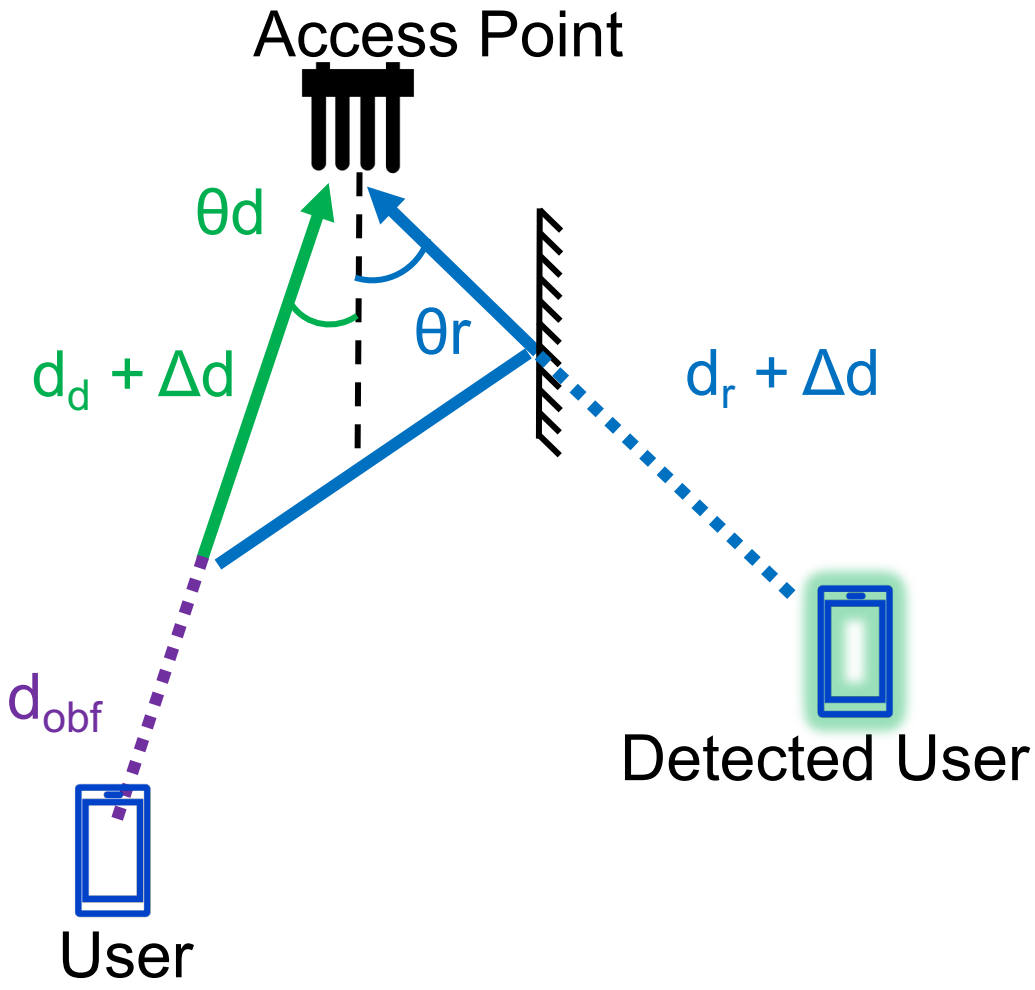


Obfuscate the Direct Path

$$d_d + \Delta d < d_r + \Delta d$$

$$d_d + \Delta d + d_{obf} > d_r + \Delta d$$

$$d_{obf} > d_r - d_d$$



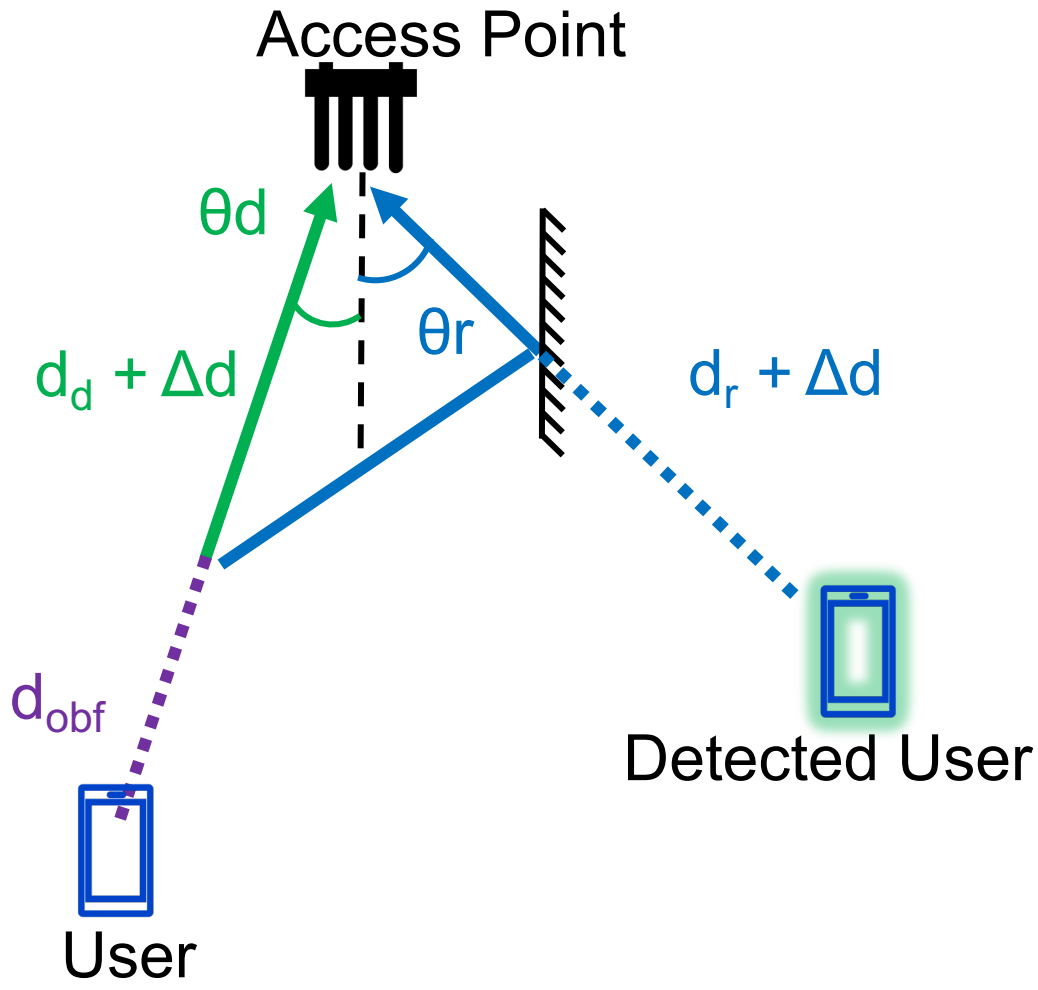
Obfuscate the Direct Path

$$d_d + \Delta d < d_r + \Delta d$$

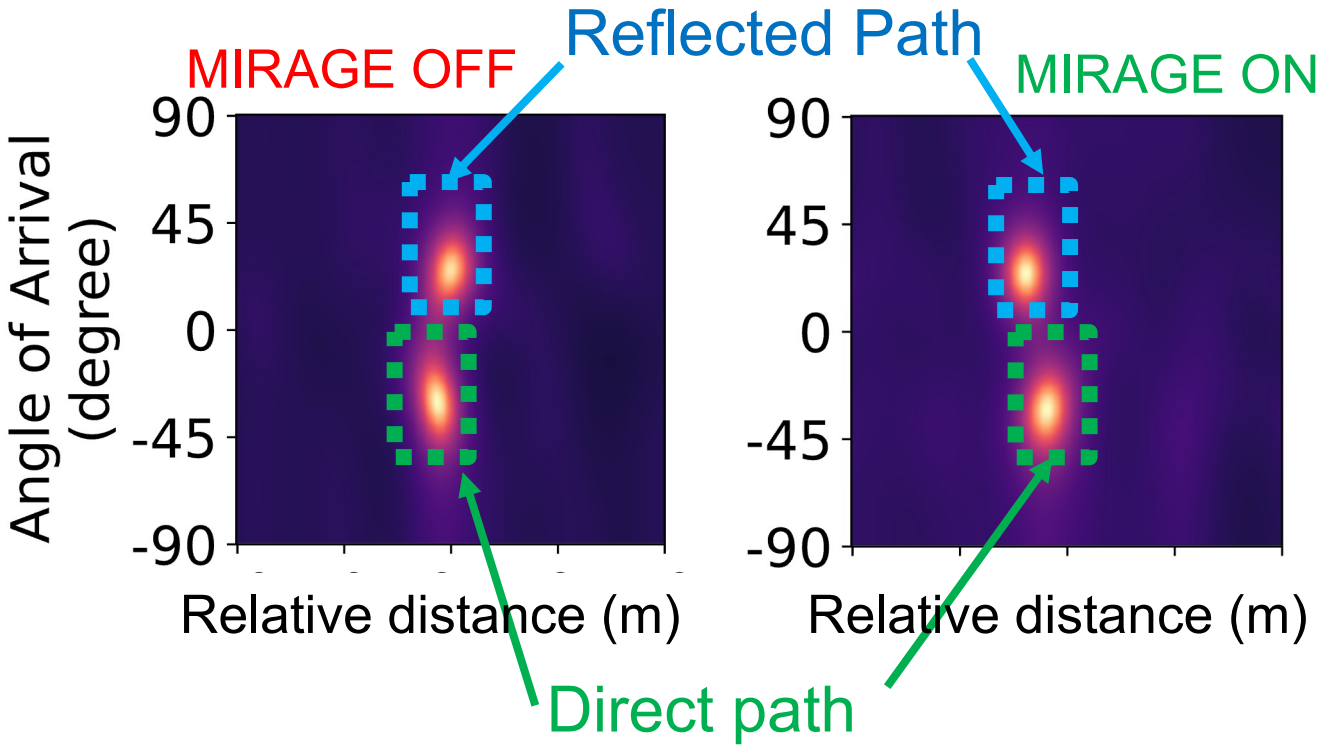
$$d_d + \Delta d + d_{obf} > d_r + \Delta d$$

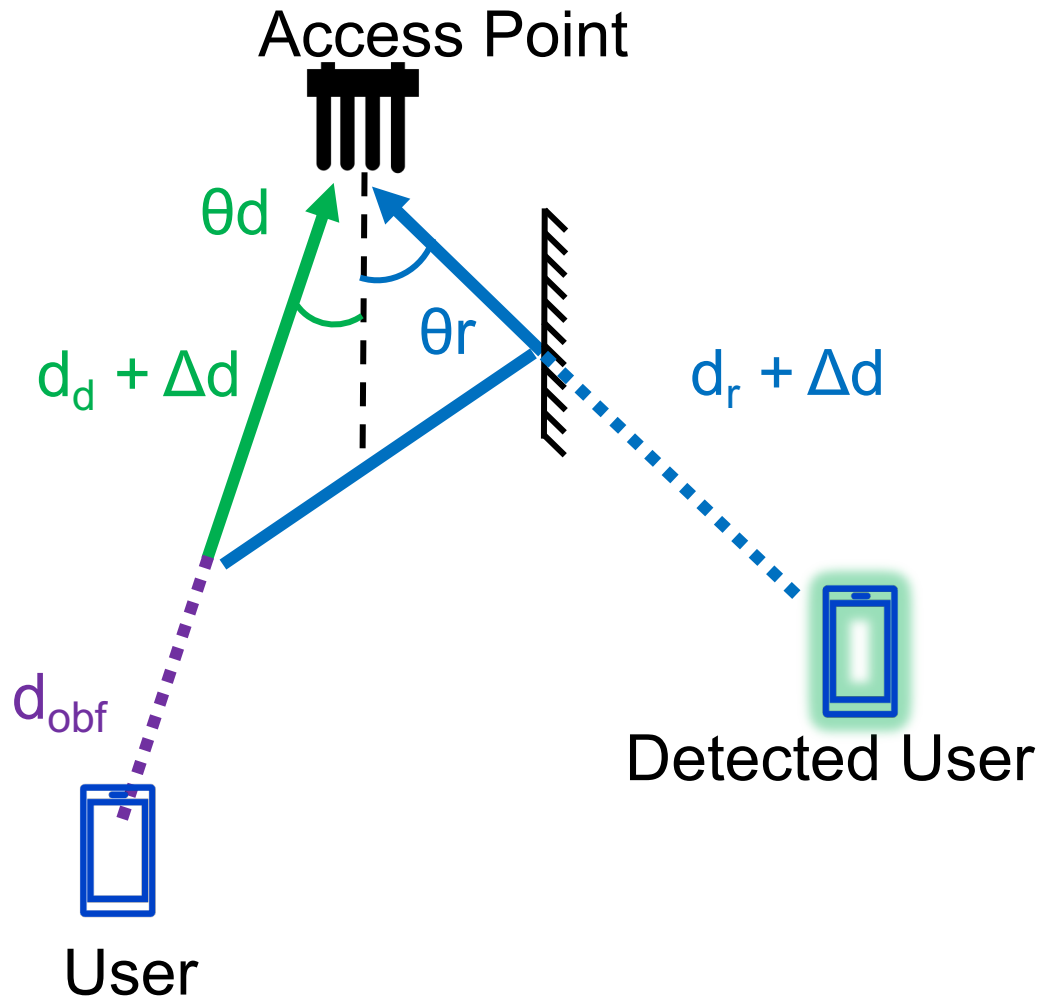
$$d_{obf} > d_r - d_d$$

Relative Distance

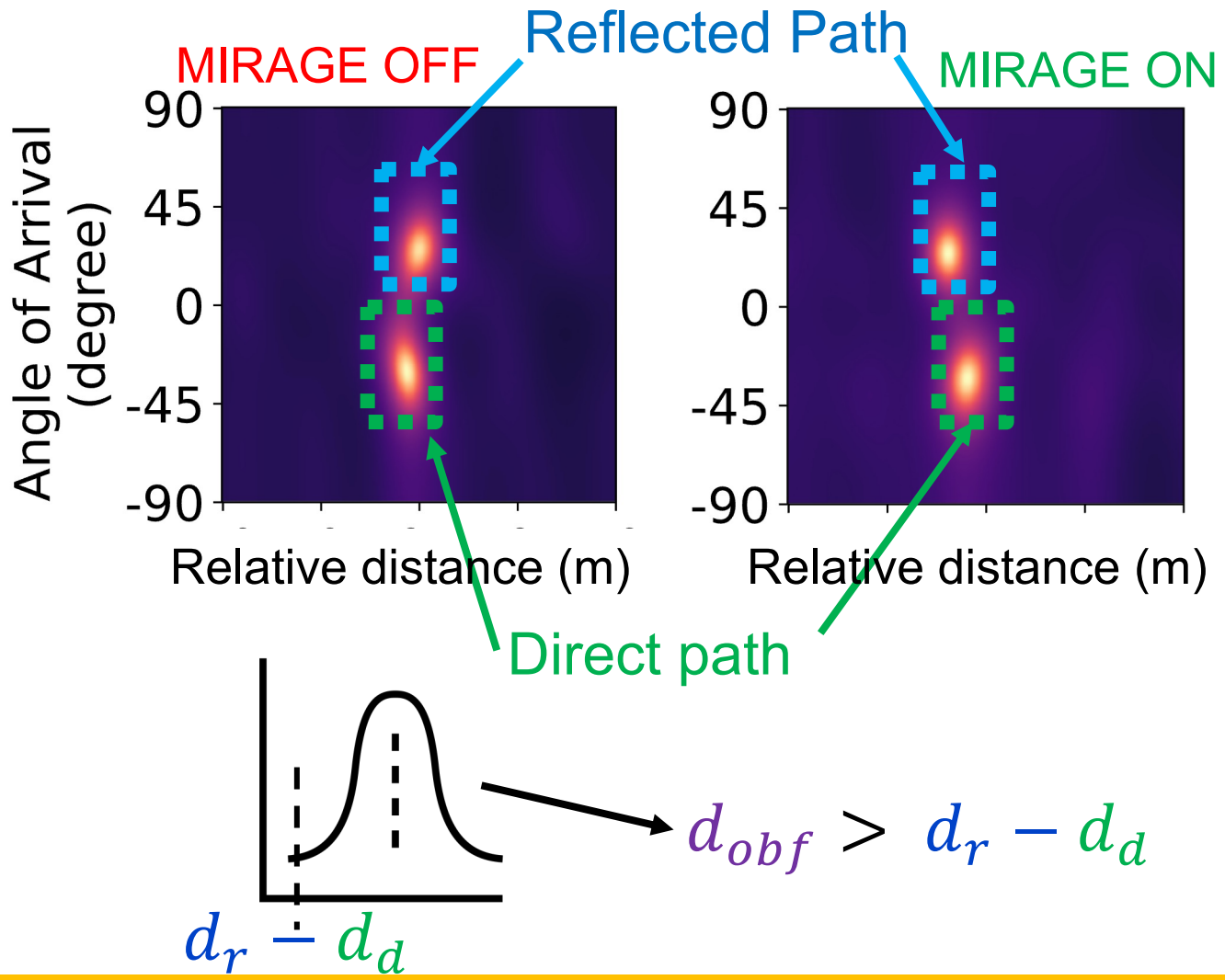


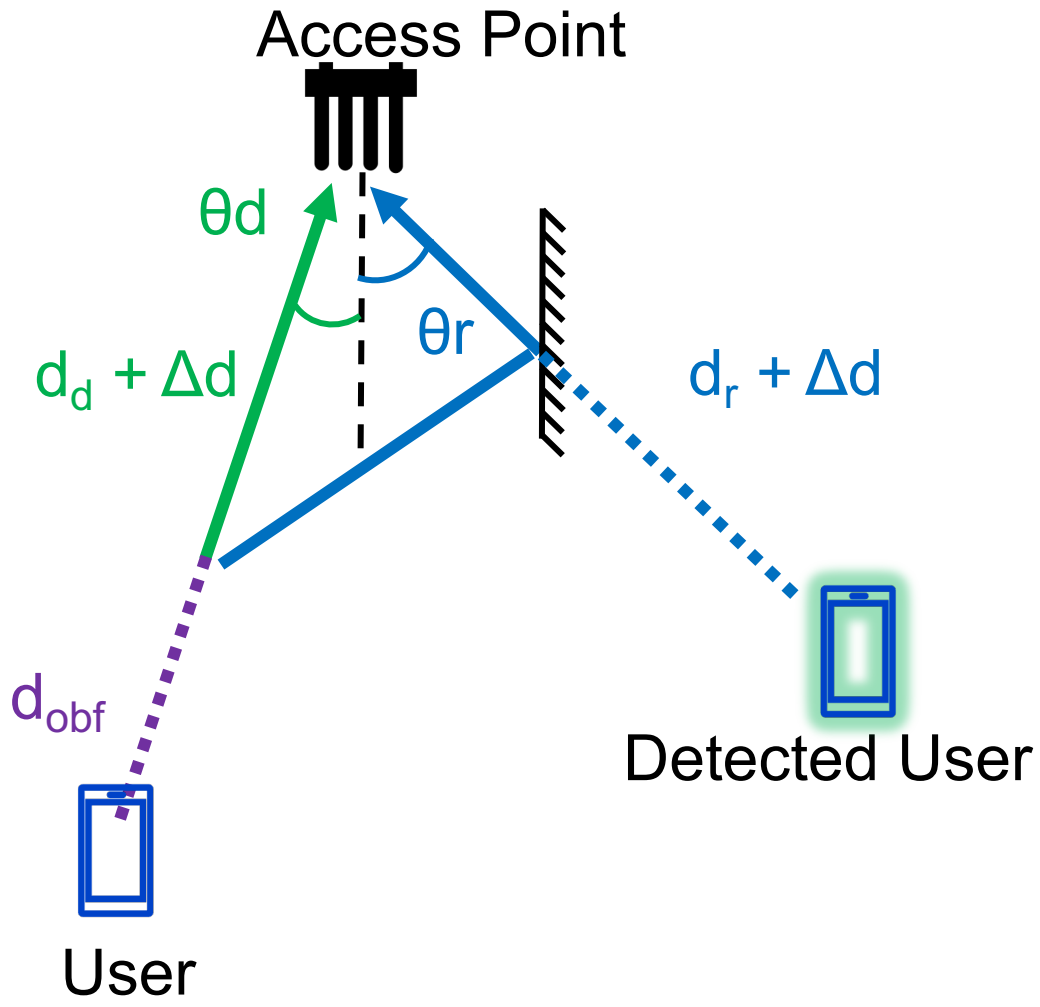
Obfuscate the Direct Path



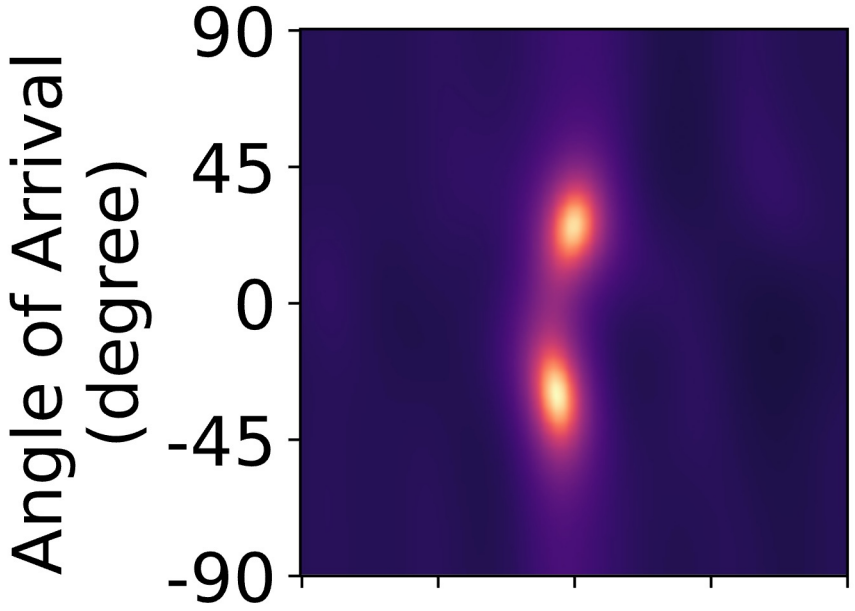


Obfuscate the Direct Path



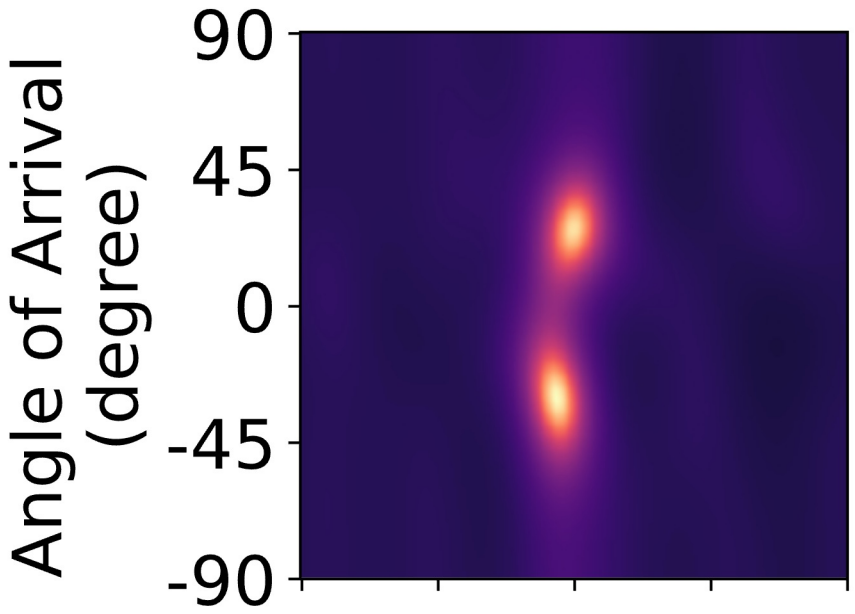


Demonstration



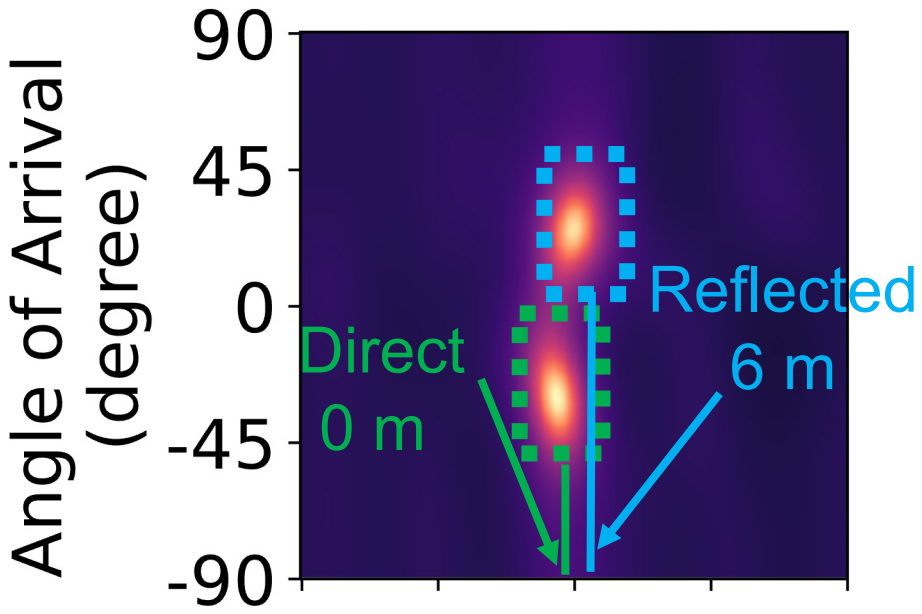
Demonstration

MIRAGE OFF | With NULLING | MIRAGE ON

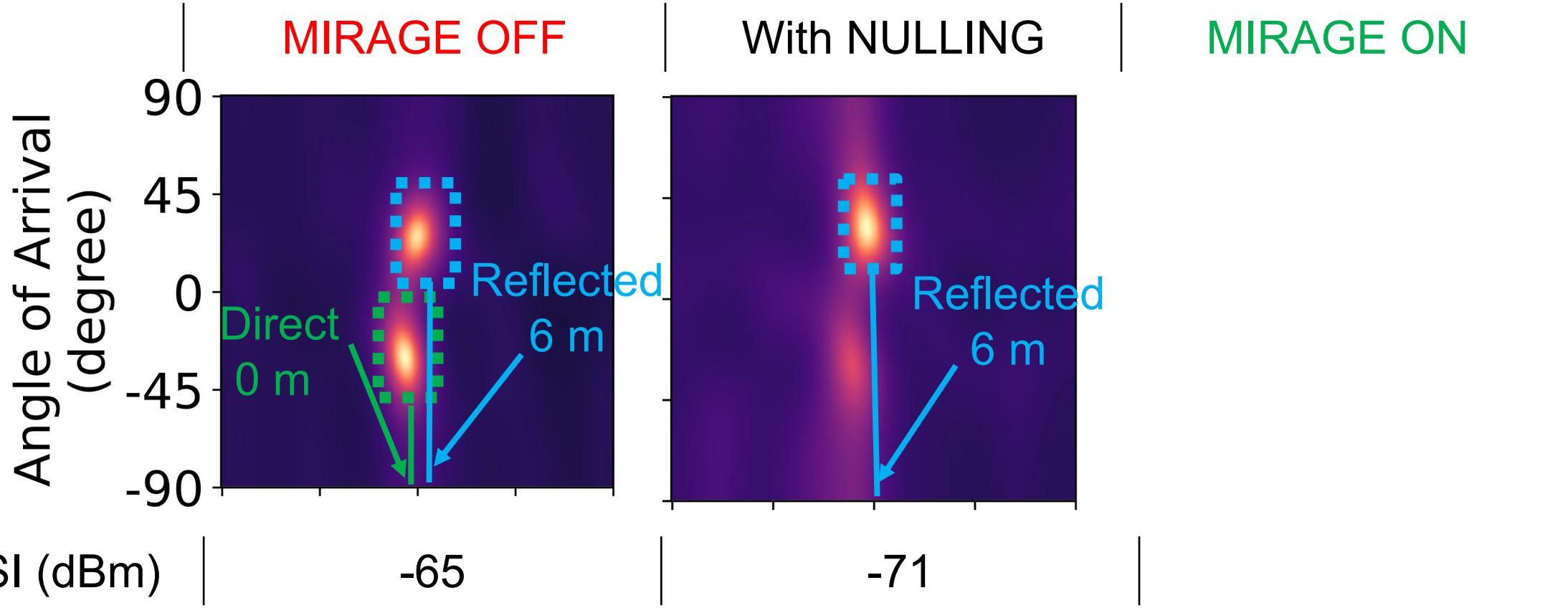


Demonstration

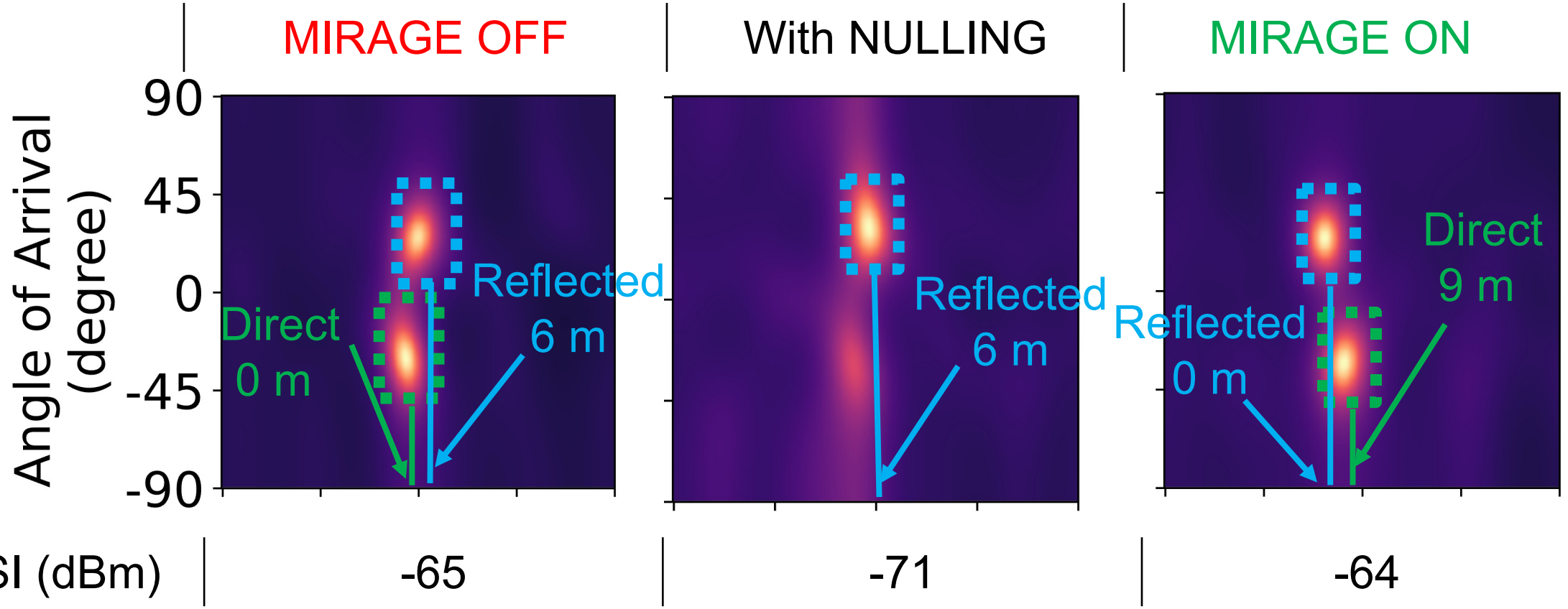
MIRAGE OFF | With NULLING | MIRAGE ON



Demonstration



Demonstration



Related Work

- **MAC address randomization**
  - MAC address randomization is shown to be easy to be broken [1]
- **IEEE 802.11mc range/distance estimate**
  - WiPeep – Mobicom'21 [3]: Attack to reveal 802.11mc range estimates
- **Signal Strength Based Systems**
  - Signal-strength based obfuscation [2]: (R2) Breaks the ongoing wireless communication
- **Modifying the wireless environment**
  - PhyCloak[4],IRShield [5],RF-Protect [6],Aegis [7]: (R2) Break the ongoing communication

[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.

MIRAGE: Satisfies our requirements

- ✓ MIRAGE:

MIRAGE: Satisfies our requirements

- ✓ MIRAGE:
  - ✓ Obfuscates the user Location. (R1)

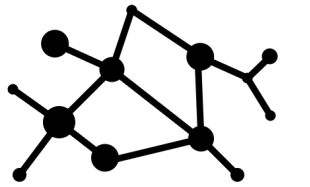
MIRAGE: Satisfies our requirements

- ✓ MIRAGE:
  - ✓ Obfuscates the user Location. (R1)
  - ✓ Maintains communication link. (R2)

MIRAGE: Satisfies our requirements

- ✓ MIRAGE:
  - ✓ Obfuscates the user Location. (R1)
  - ✓ Maintains communication link. (R2)
  - ✓ Even with the knowledge of MIRAGE, attacker will still be confused amongst the N-multipaths. (R3)

UC San Diego
JACOBS SCHOOL OF ENGINEERING
Electrical and Computer Engineering



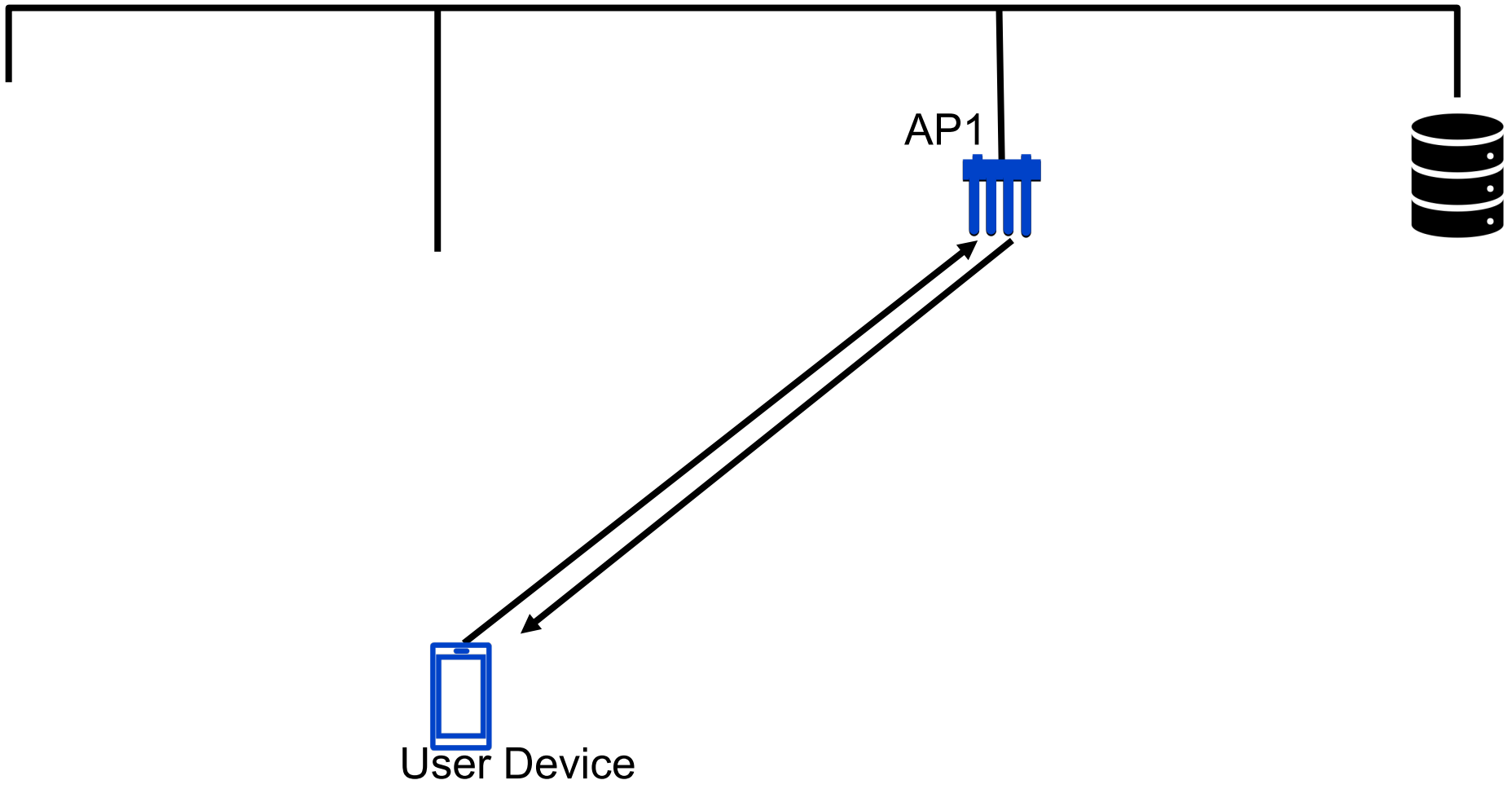
WCSNG
Wireless Communications
Sensing and Networking

Users are closer than they appear

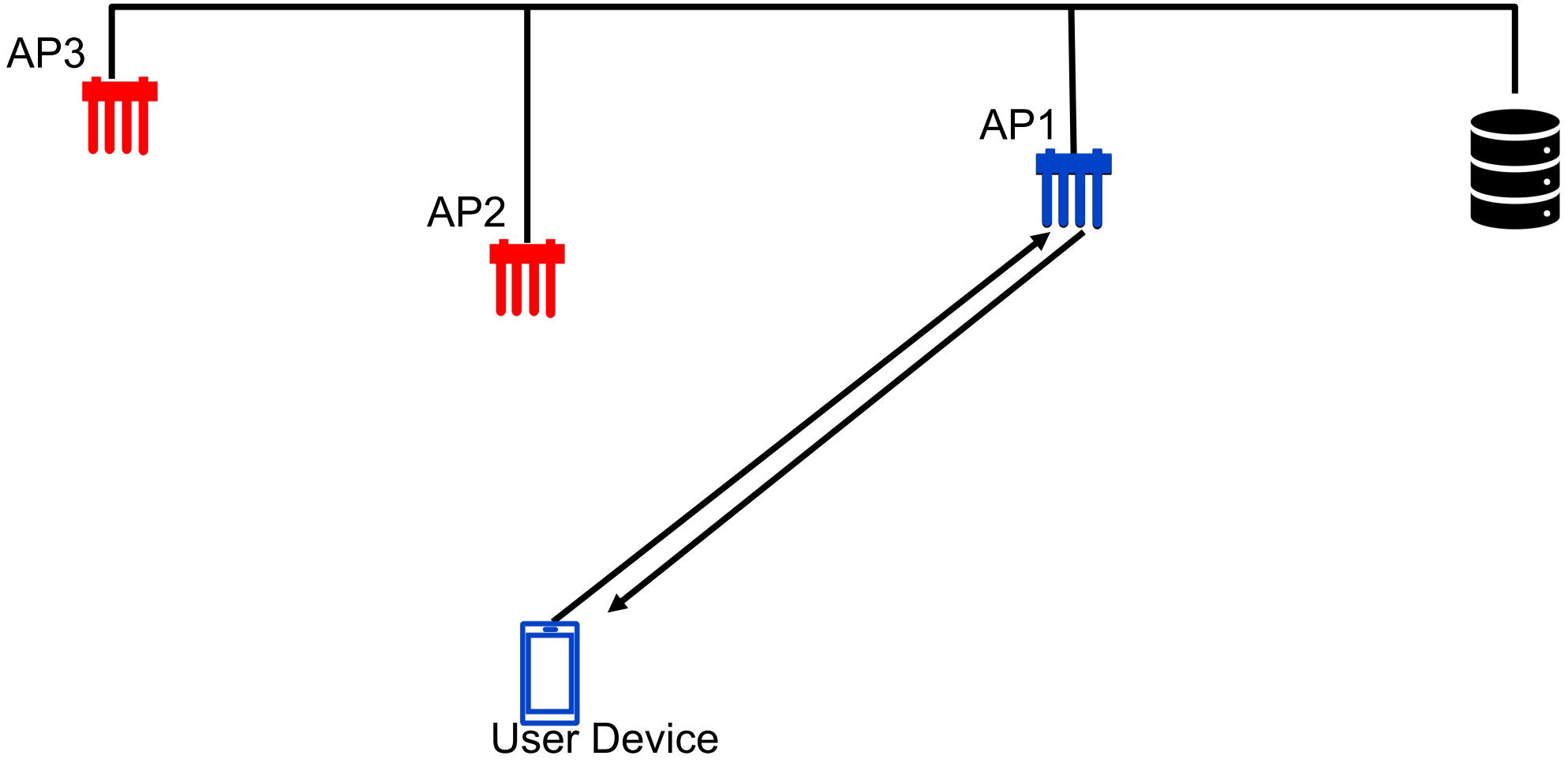
MIRAGE: Protecting User Locations from Wi-Fi APs

Challenges and Open Problems

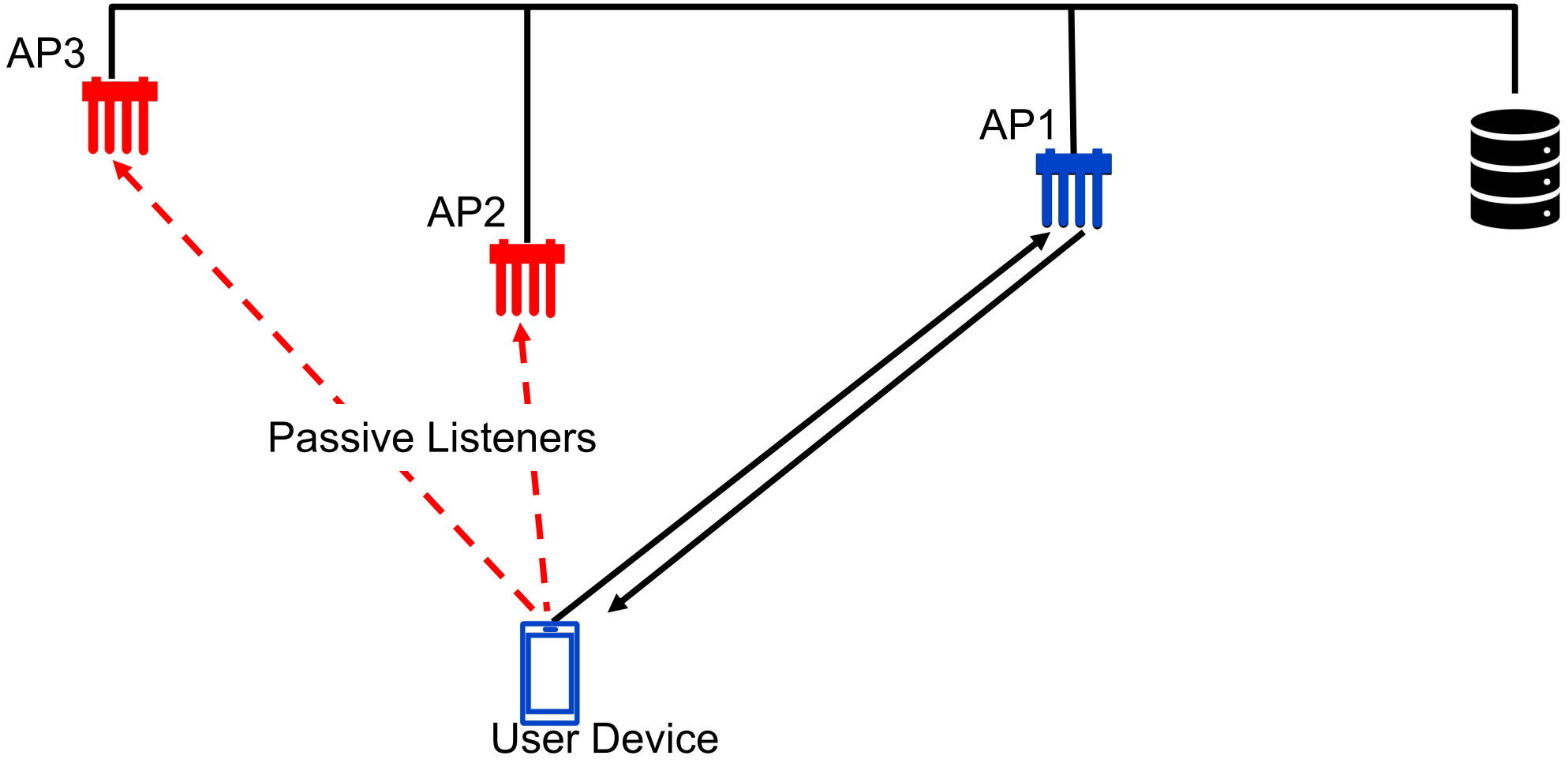
Multiple Collaborative Wi-Fi APs



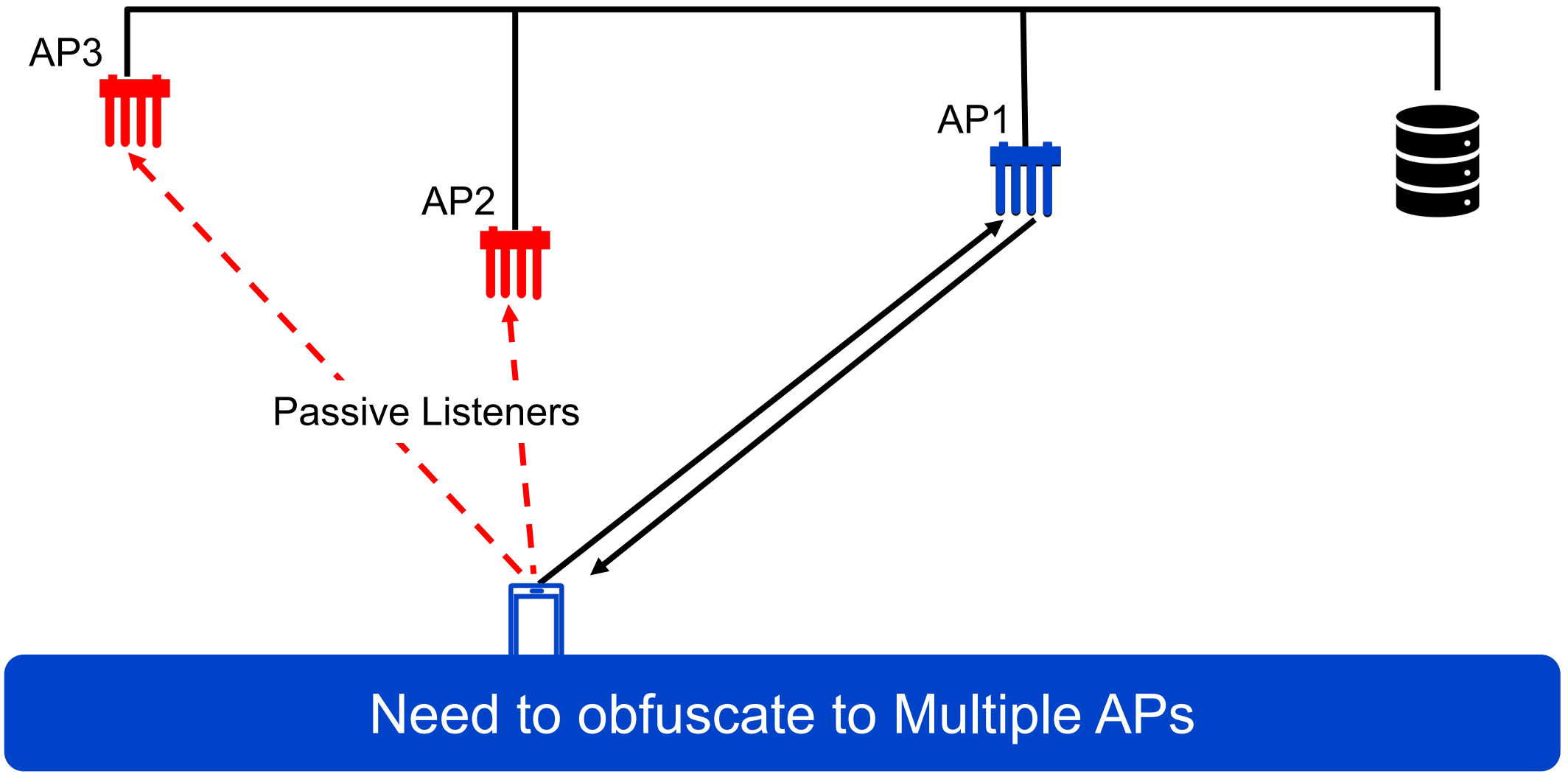
Multiple Collaborative Wi-Fi APs



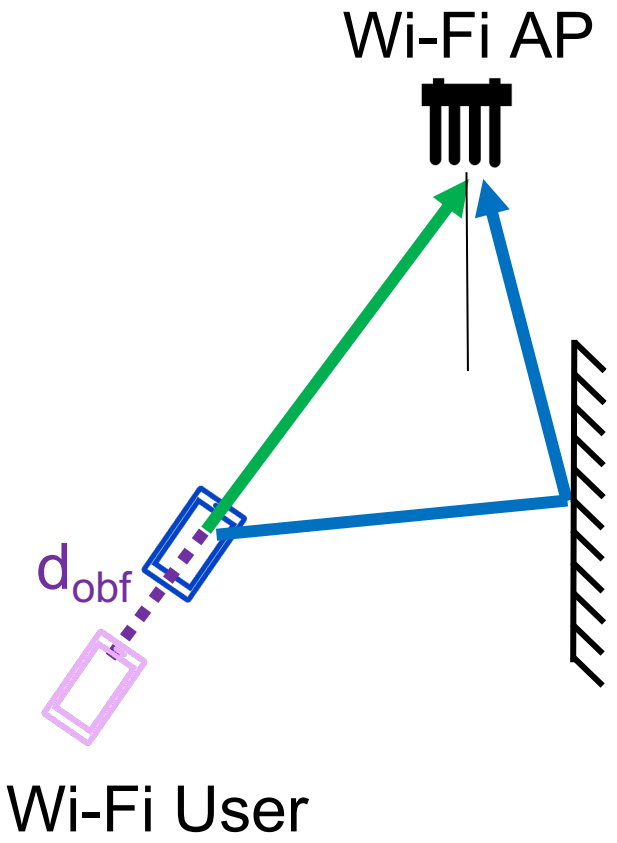
Multiple Collaborative Wi-Fi APs



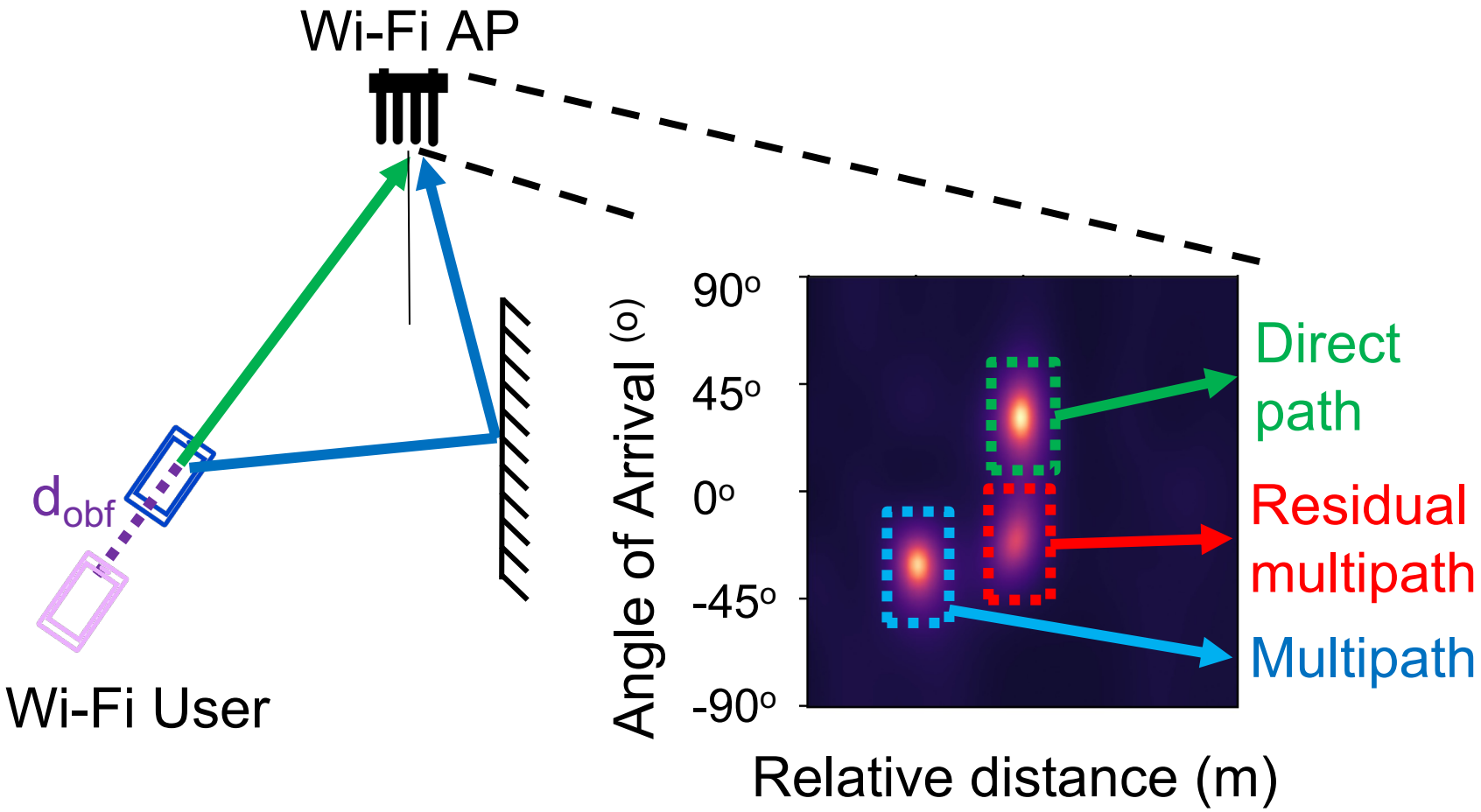
Multiple Collaborative Wi-Fi APs



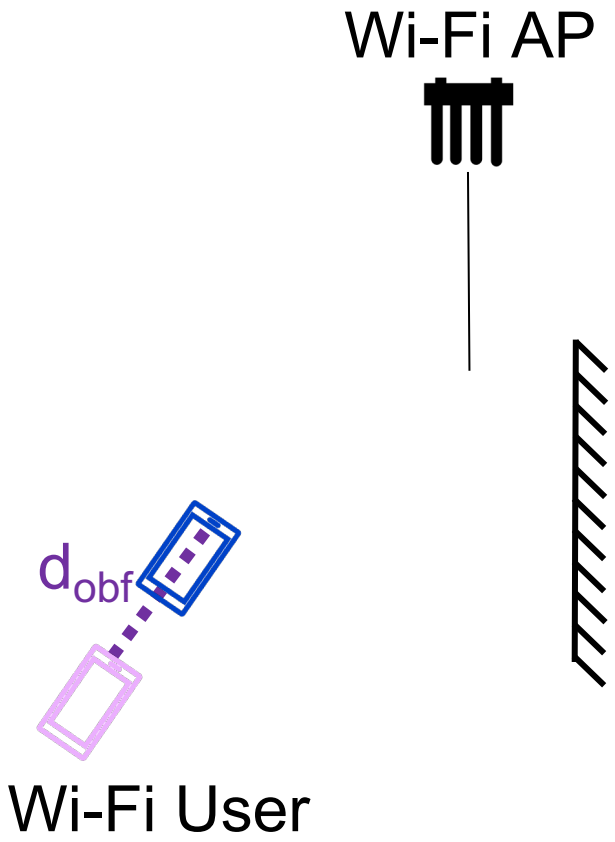
Corner case: MIRAGE reveals actual user AoA



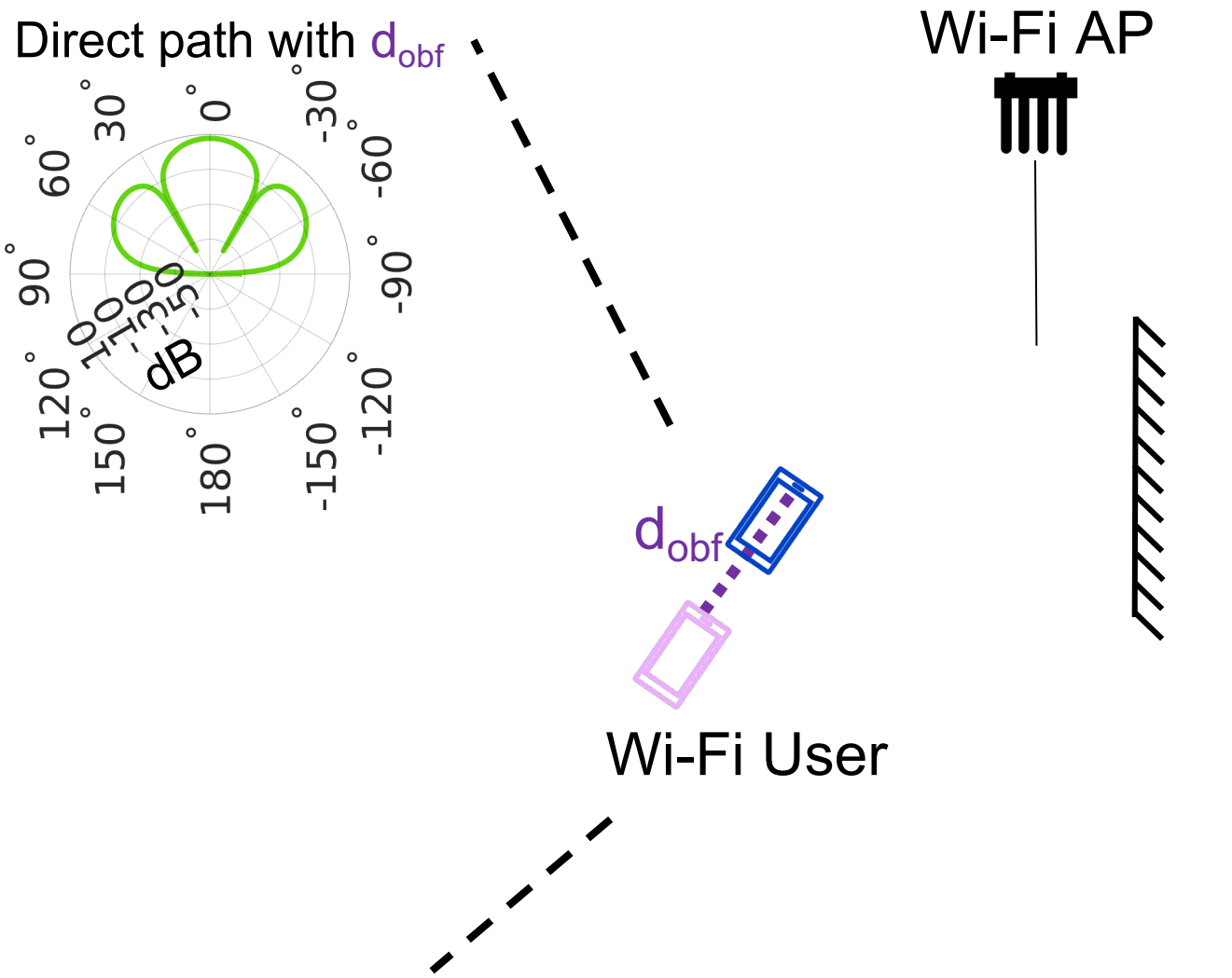
Corner case: MIRAGE reveals actual user AoA



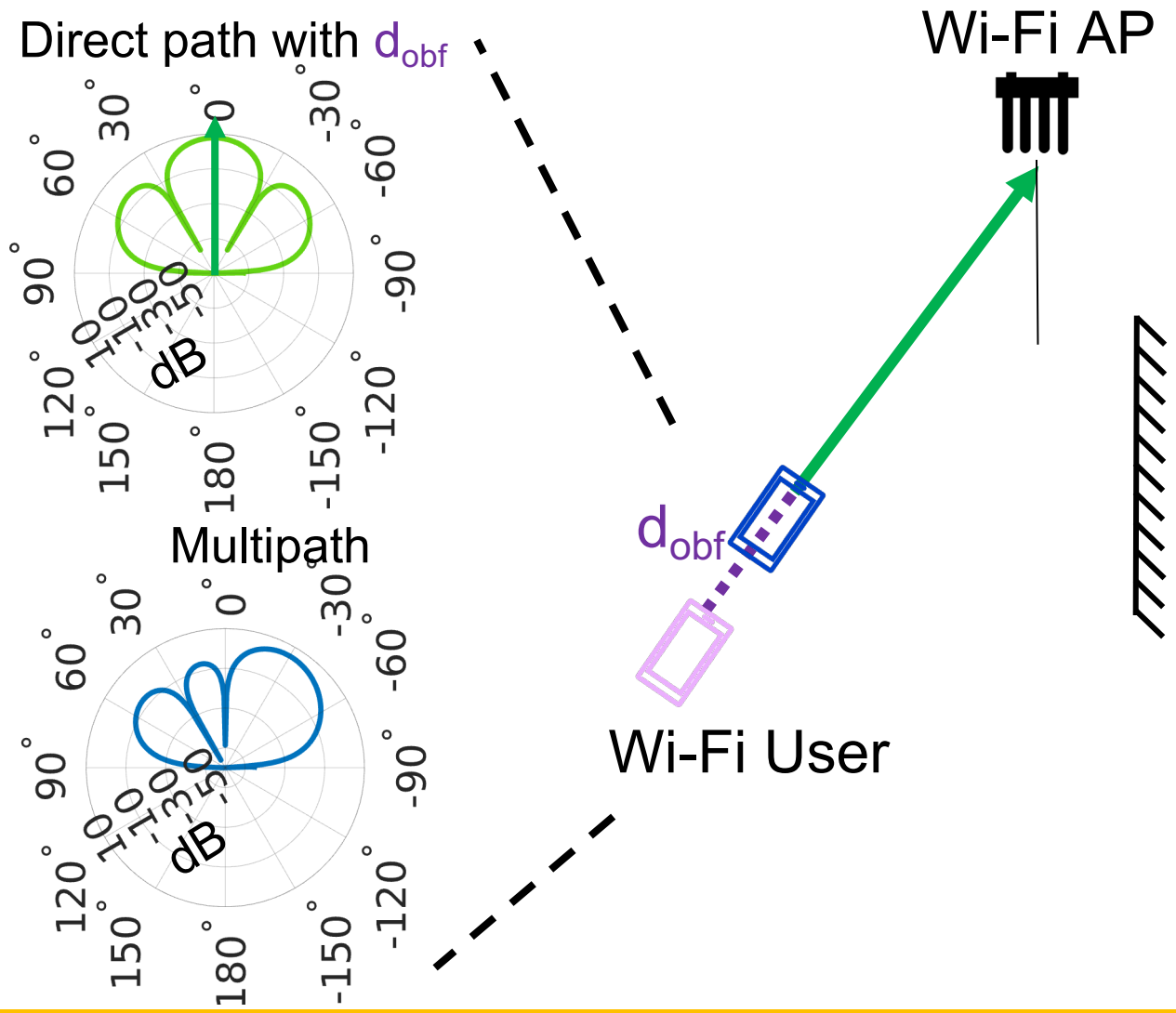
Leakage from Direct Path along reflected path



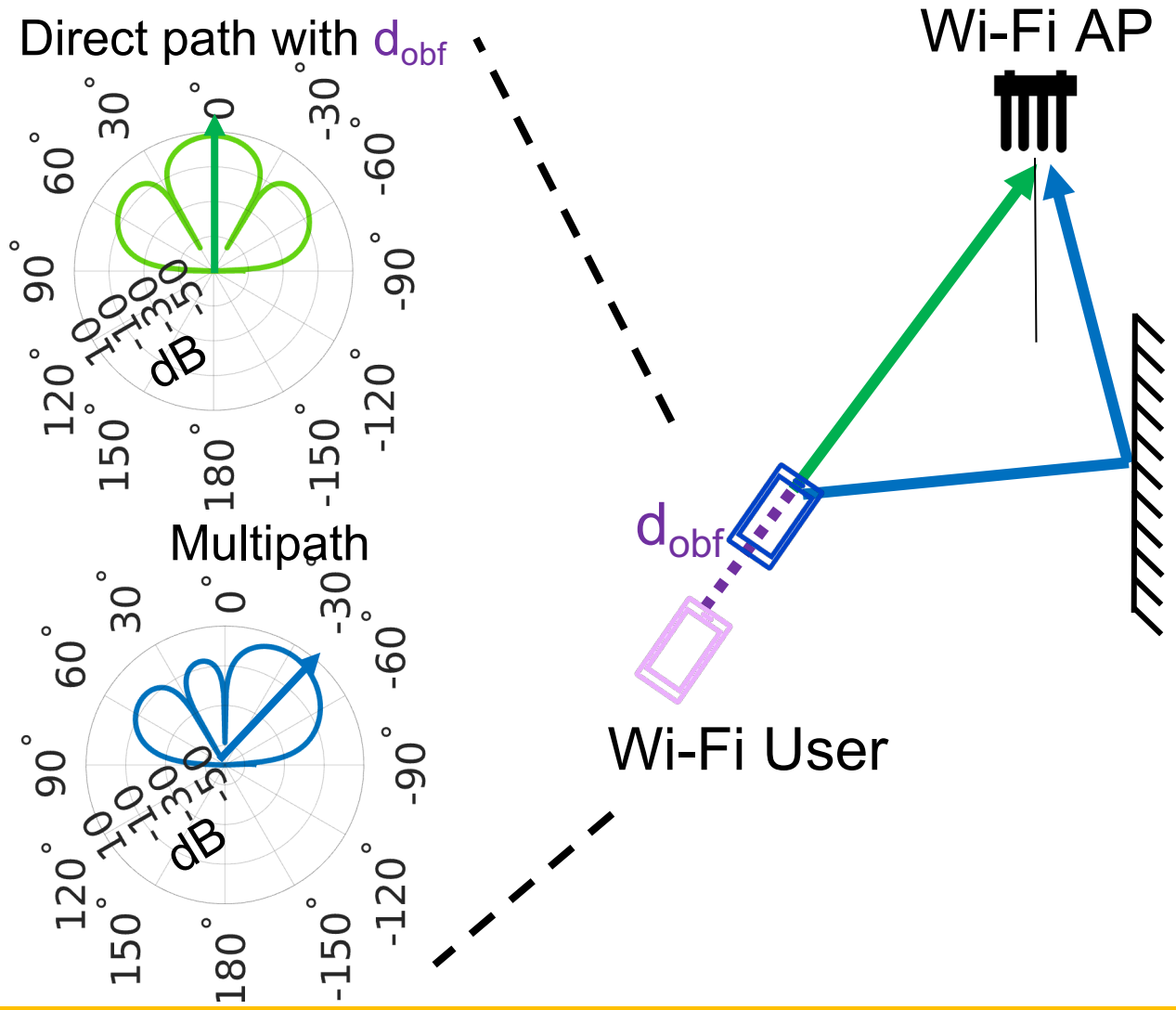
Leakage from Direct Path along reflected path



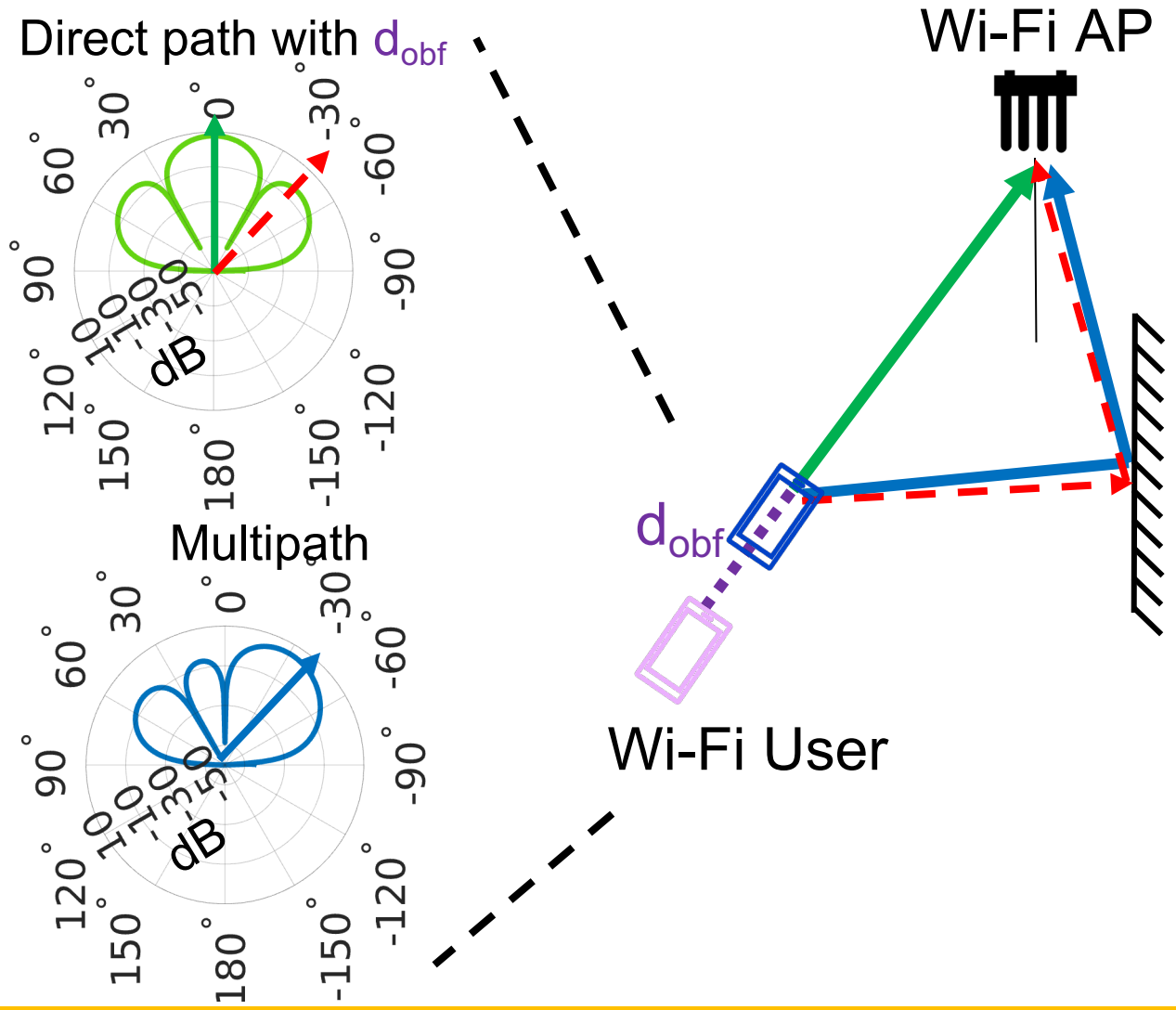
Leakage from Direct Path along reflected path



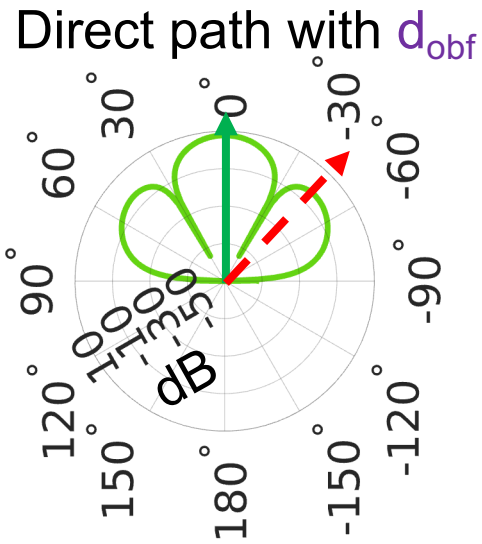
Leakage from Direct Path along reflected path

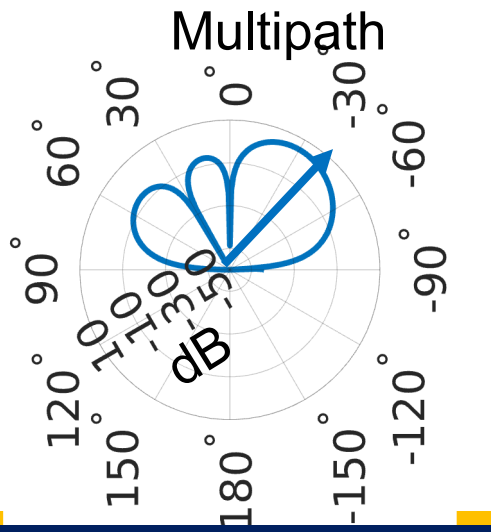


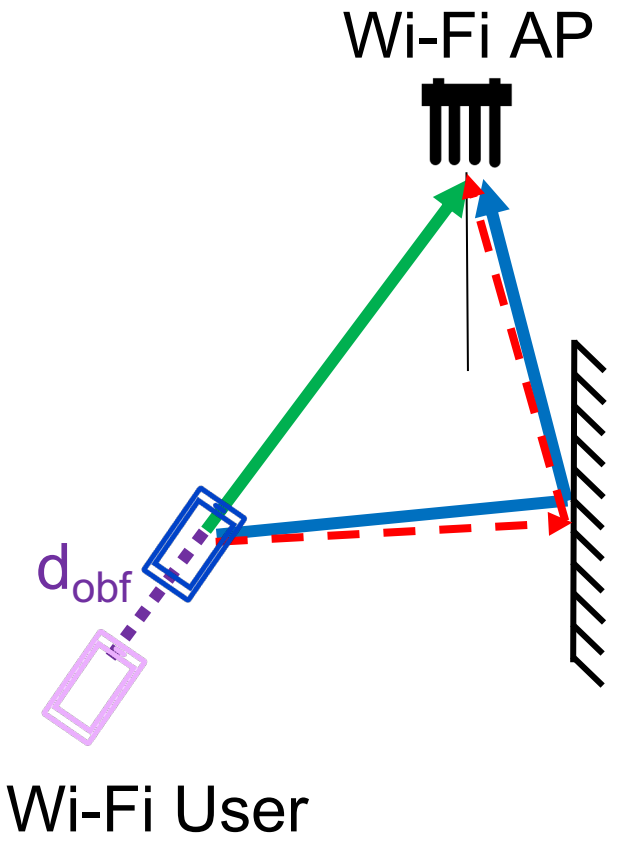
Leakage from Direct Path along reflected path



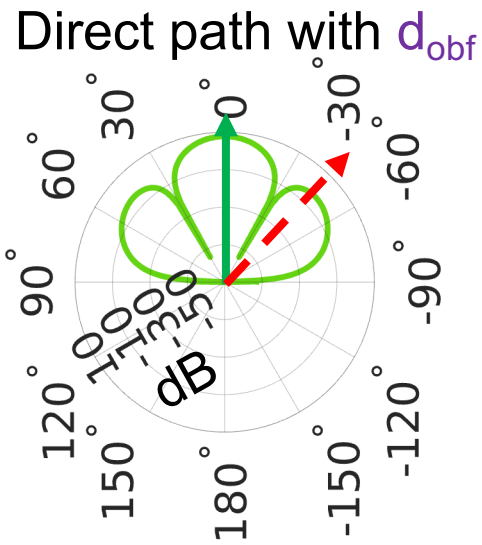
Beamforming+Nulling Capability

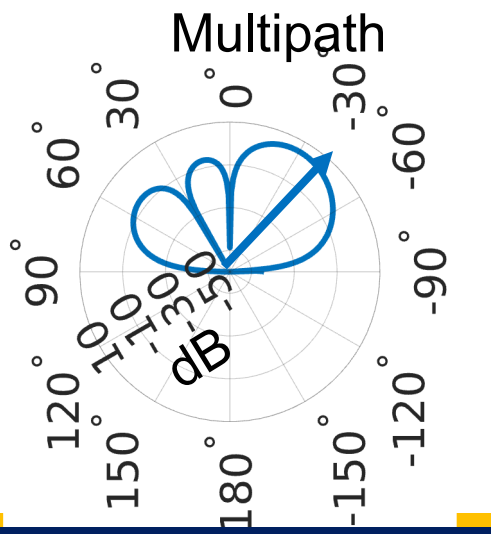


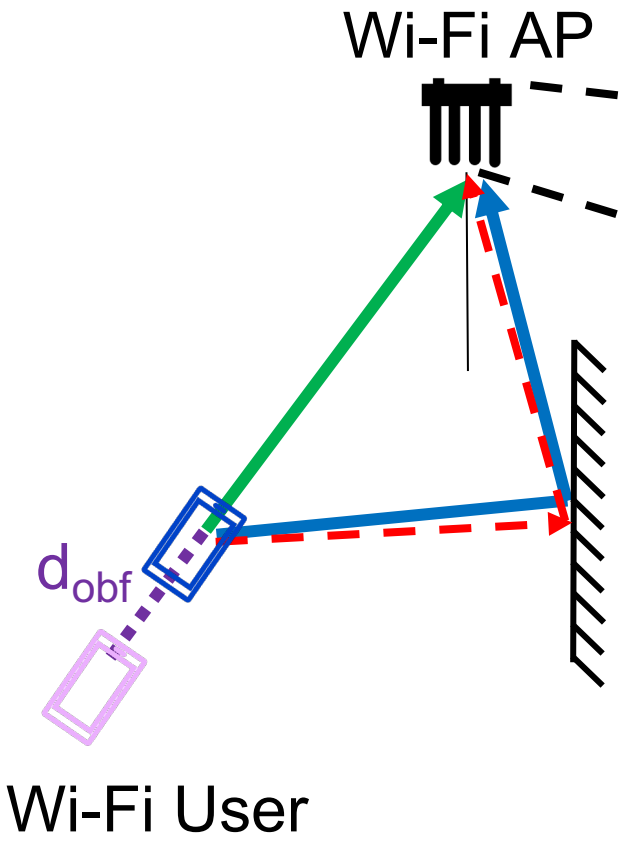


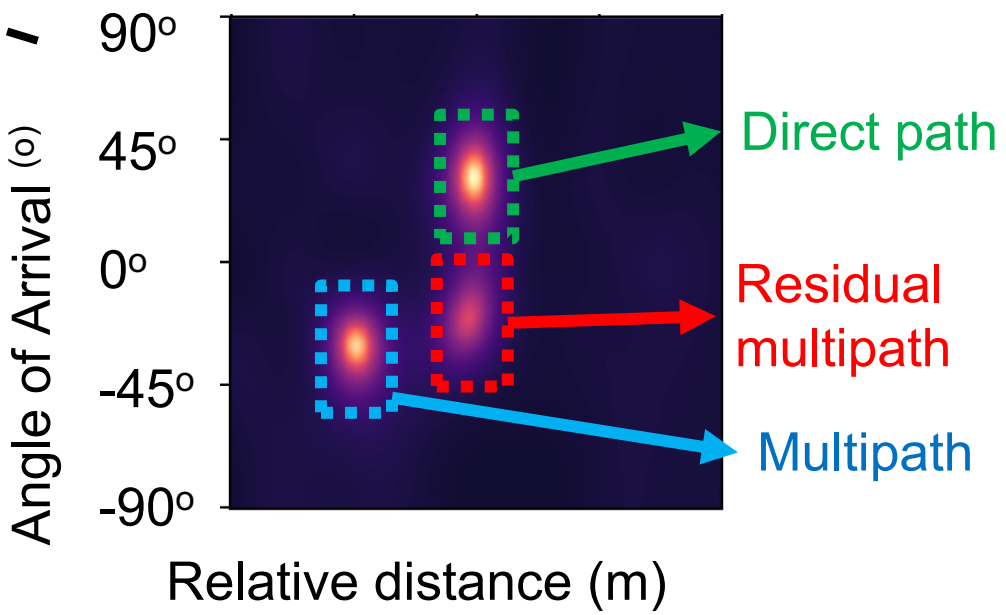


Beamforming+Nulling Capability

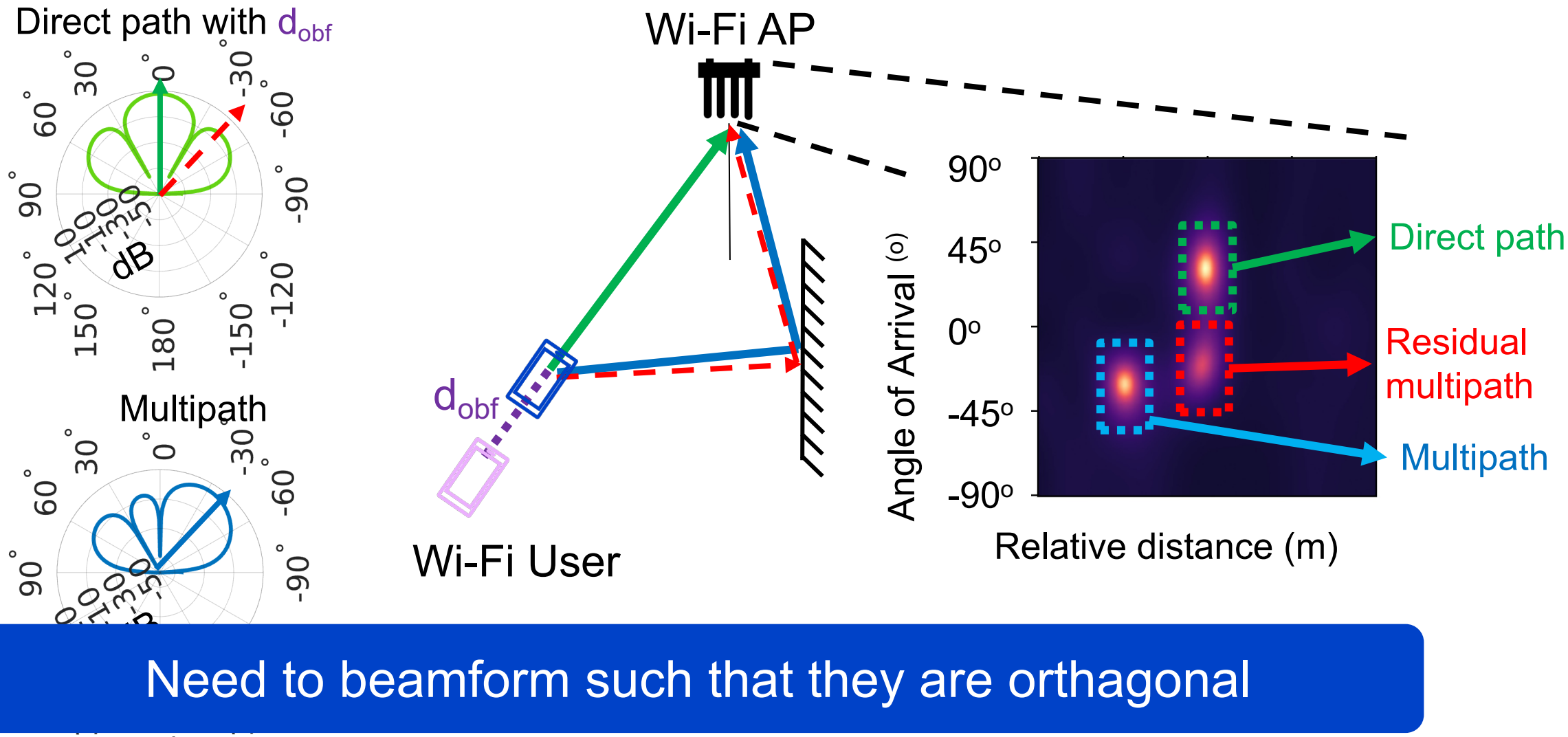






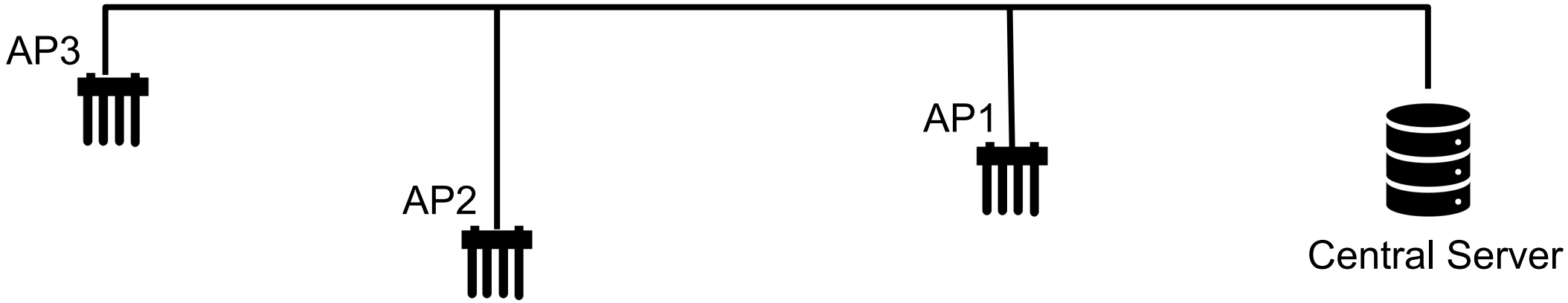


Beamforming+Nulling Capability

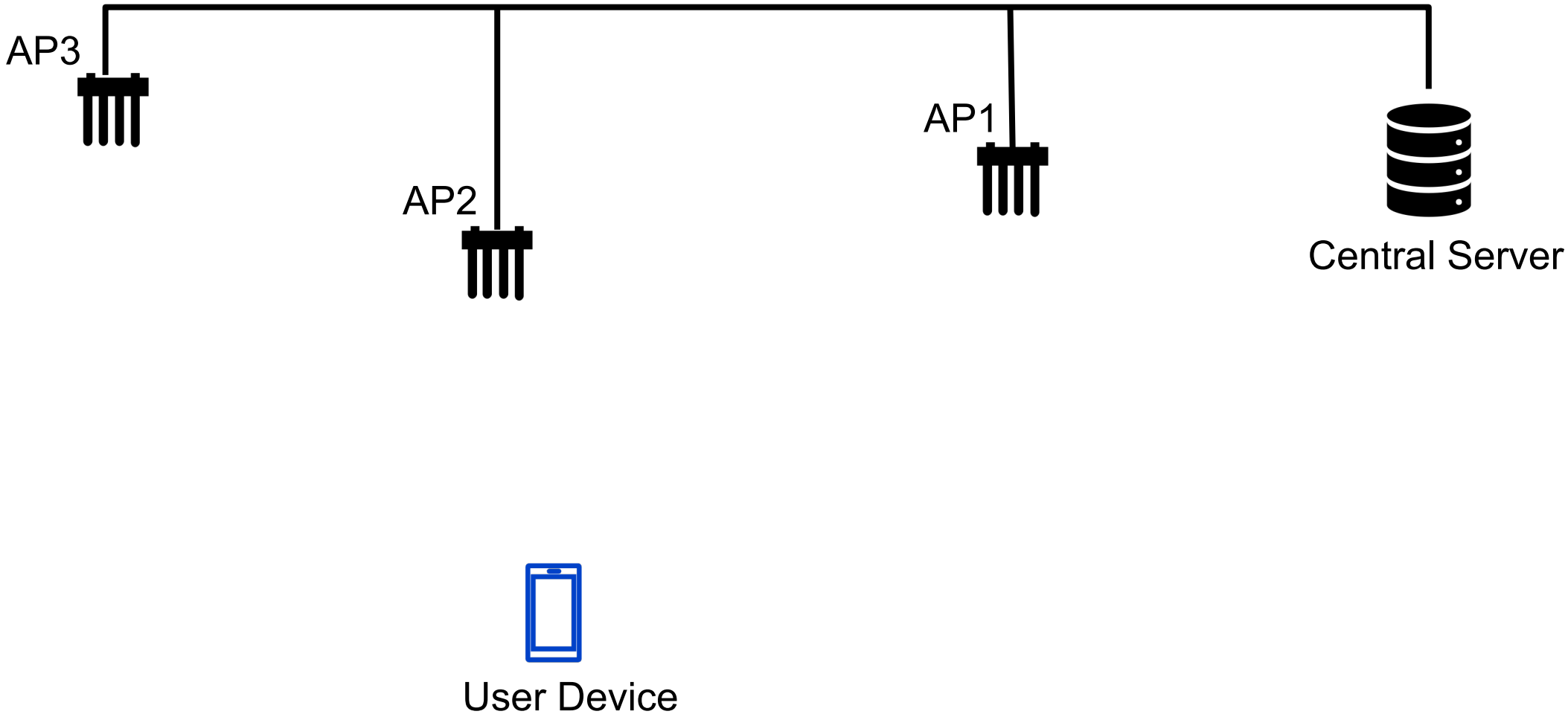


Need to beamform such that they are orthagonal

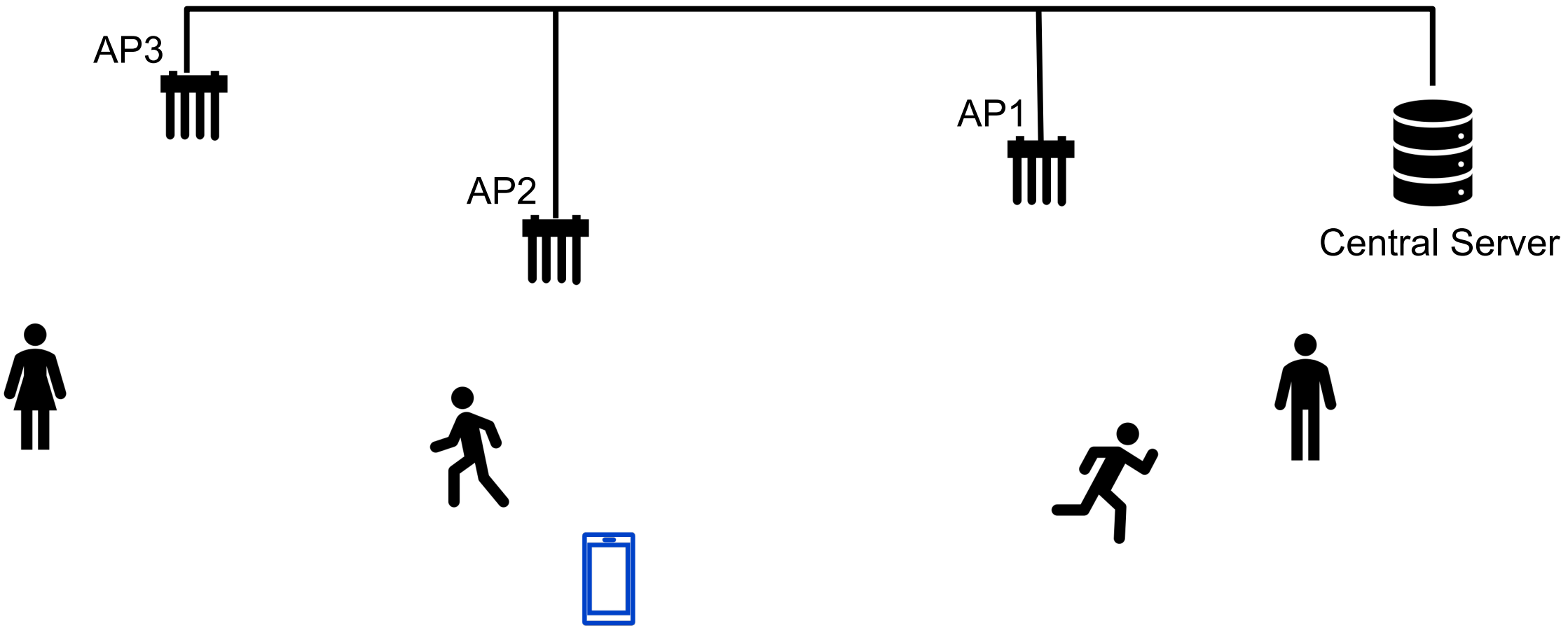
Dynamic User and/or Environment



Dynamic User and/or Environment



Dynamic User and/or Environment



Need to model Dynamic multipath

MIRAGE: Protecting User Locations from Wi-Fi APs

- ✓ MIRAGE:
  - ✓ Obfuscates the user Location (R1)
  - ✓ Maintains communication link (R2)
  - ✓ Even with the knowledge of MIRAG, attacker will get N-location for N-multipaths in the environment (R3)

Contact: roshana@ucsd.edu aarun@eng.ucsd.edu w5sun@ucsd.edu

Scan me!

MIRAGE: Protecting User Locations from Wi-Fi APs

- ✓ MIRAGE:
  - ✓ Obfuscates the user Location (R1)
  - ✓ Maintains communication link (R2)
  - ✓ Even with the knowledge of MIRAG, attacker will get N-location for N-multipaths in the environment (R3)
- ❑ Challenges and Open Problems
  - ❑ Improving User Location Obfuscation
  - ❑ Multiple Collaborative Aps
  - ❑ Dynamic User and/or Multipath Scenarios

Contact: roshana@ucsd.edu aarun@eng.ucsd.edu w5sun@ucsd.edu

Scan me!