Et Tu Alexa? When Commodity WiFi Devices Turn into Adversarial Motion Sensors

Yanzi Zhu†, Zhujun Xiao*, Yuxin Chen*, Zhijing Li†, Max Liu*, Ben Y. Zhao*, Haitao Zheng*
†University of California, Santa Barbara: {yanzi, zhijing}@cs.ucsb.edu
*University of Chicago: {zhujunxiao, yxchen, maxliu, ravenben, htzheng}@cs.uchicago.edu

***Abstract*—Our work demonstrates a new set of silent reconnaissance attacks, which leverages the presence of commodity WiFi devices to track users inside private homes and offices, without compromising any WiFi network, data packets, or devices. We show that just by sniffing existing WiFi signals, an adversary can accurately detect and track movements of users inside a building. This is made possible by our new signal model that links together human motion near WiFi transmitters and variance of multipath signal propagation seen by the attacker sniffer outside of the property. The resulting attacks are cheap, highly effective, and yet difficult to detect. We implement the attack using a single commodity smartphone, deploy it in 11 real-world offices and residential apartments, and show it is highly effective. Finally, we evaluate potential defenses, and propose a practical and effective defense based on AP signal obfuscation.**

I. Introduction

With near-ubiquitous deployment of WiFi-enabled smart devices (*e.g.*, security cameras, voice assistants, and smart appliances), our homes and offices are filled with many WiFi devices[1]. The ubiquity of these devices and their sheer density means that they will fill the air around us with radio frequency (RF) signals, wherever we go.

Unfortunately, the RF signals emitted by these devices pose a real security and privacy risk to all of us. They are constantly interacting with (*e.g.*, reflecting off) our bodies, carrying information about our location, movement and other physiological properties to anyone nearby with sufficient knowledge and curiosity. In this work, we explore a new set of passive reconnaissance attacks that leverages the presence of *ambient WiFi signals* to monitor users in their homes and offices, even when the WiFi network, data packets, and individual devices are completely secured and operating as expected. We show that by just sniffing existing WiFi signals, an adversary outside of the target property can accurately detect and track movements of any users down to their individual rooms, regardless of whether they are carrying any networked devices.

We believe this is the first in a new class of silent reconnaissance attacks that are notable because of their passive nature and general applicability. This attack can be highly effective, incurs low cost (only cheap commodity hardware), and yet remains *undetectable*. The attacker does not need to compromise/access the WiFi network or individual devices, decode packets or transmit any signals. All they need is to place a single, off-the-shelf, minimally equipped WiFi receiver outside of the target property. This attacker receiver only needs a *single* antenna, and simply measures the signal strength of existing WiFi signals, without decoding any packets.

Unaddressed, these reconnaissance attacks put our security and privacy at significant risk. The ability for an attacker to continuously and automatically scan, detect and locate humans behind walls at nearly no cost and zero risk (*e.g.* attacker waits for notifications remotely) will enable attackers to launch strong physical attacks and commit serious crimes. Such threat broadly applies to our homes, businesses, government facilities and many others. Examples include burglary to homes and offices, kidnapping and assault of targets in their homes, "casing" a bank prior to robbery, and even planning attacks against government agencies.

Why WiFi sensing? We note that there are some simple approaches to inferring user presence that do not require the use of sophisticated RF sensing. For example, attackers could infer user presence by observing lighting or acoustic conditions inside an area, or use thermal imaging. These attacks are well understood and easily disrupted by time-controlled lighting or sound systems [3], or insulated walls designed to prevent heat leakage and naturally block thermal imaging [1]. Finally, attackers can infer user presence from increased WiFi network traffic. Yet this is highly unreliable, as growth of IoT devices increases traffic levels in the absence of users. It is also easily thwarted using cover traffic [15].

Instead, we describe a new class of physical reconnaissance attacks enabled by inherent properties of WiFi signal propagation: 1) user movement near a WiFi transmitter changes its signal propagation in a way that can be observed by nearby receivers, and 2) walls and buildings today are not built to insulate against WiFi signals, thus signals sent by devices inside a property can often be overheard by outside receivers. Leveraging these, we design the attack such that, whenever a WiFi device transmits signals, it unknowingly turns into a tracking device for our attack. In this context, our attack could be viewed as an adversarial analogy to WiFi-based device-free human sensing (*e.g.*, see-through-wall systems that actively transmit customized RF signals towards the target [14]). Yet our attack differs significantly (§II), because we use a novel model on multipath signal dynamics to remove dependence on active transmissions (only passive sensing), customized

[1]The worldwide number of WiFi-enabled IoT devices is expected to reach 5 billion by 2025 [6], and the number of WiFi connected devices will reach 22.2 billion by 2021 [9].

Network and Distributed Systems Security (NDSS) Symposium 2020
23-26 February 2020, San Diego, CA, USA
ISBN 1-891562-61-4
https://dx.doi.org/10.14722/ndss.2020.23053
www.ndss-symposium.org

hardware (only a commodity, single antenna receiver), and knowing precise locations of WiFi devices inside the property.

Motion detection via multipath signal dynamics. The core of our attack is a new model on signal dynamics that links together human motion near WiFi transmitters and variance of multipath signal propagation seen by a sniffer outside of the property. Specifically, when a human target moves (*e.g.*, sitting down, walking, opening/closing doors) near a WiFi device x, the motion changes the multipath signal propagation from x to the attacker sniffer S. Our new signal model allows S to accurately capture such signal dynamics and use them to pinpoint the target to her specific room. The more WiFi devices inside the property, the more accurate the tracking becomes.

Our proposed attack does not assume any prior knowledge of the WiFi network and devices inside the target property, including their locations. Our attack can discover devices and estimate their coarse locations using their WiFi signals, and the attack continues to function even if these devices are relocated.

We build a complete prototype of the attacker system on commodity smartphones, and experimentally show that the attack (using a single smartphone) is not only highly accurate (detecting and localizing users to an individual room), but also highly general (effective across a wide range of 11 different physical settings, including both office buildings and residential apartments).

Defense via AP-based signal obfuscation. We explore robust defenses against our proposed attack and other passive sensing attacks. We consider four immediate defenses: reducing leakage by geo-fencing and rate limiting, signal obfuscation by MAC randomization, and power randomization at WiFi devices, and find that they are either impractical or ineffective. We then propose a practical alternative using *AP-based signal obfuscation*, where the WiFi Access Point actively injects customized cover signal for its associated devices. This defense effectively creates noise to the signal measurements, such that the attacker is unable to identify change due to human motion. Our defense is easy to implement, incurs no changes to devices other than the AP, but reduces the human detection rate to 47% while increasing the false positive rate to 50%. Such ambiguity renders the attack useless in practice.

In the rest of the paper, we describe our efforts to understand the feasibility, challenges, and defenses surrounding the proposed attack. In short, our key contributions include:

- We identify a low-cost, undetectable human sensing attack using just a single sniffer with a single antenna, and design a new multipath signal variance model for motion detection.
- We prototype the attacker system on a commodity smartphone and validate the attack in real-world settings.
- We propose and evaluate a practical and effective defense using AP-based signal obfuscation.

Limitations. Currently, our attack detects human presence in each room over time by detecting and localizing targets to individual rooms. It is unable to identify fine-grained features such as speed, activity type and user identity, or separate humans from large animals. Despite such limitations, our work identifies a realistic, low-cost, and undetectable reconnaissance attack using passive WiFi sensing. We hope our work brings more attention to this important and understudied topic.

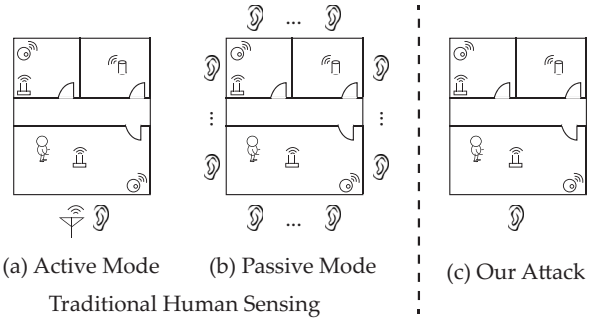


Fig. 1. Traditional human sensing designs either (a) relies on active transmissions by (customized) attacker devices, or (b) deploys one or more advanced sniffers (laptops/USRPs) with multiple antennas; (c) Our attack uses a single smartphone (with a single antenna) as the passive sniffer, and turns commodity WiFi devices inside the property as motion sensors.

II. Background: Device-free Human Sensing

Some details of adversarial sensing attacks are reminiscent of the problem of "device-free human sensing." A natural question is: *can we simply reuse existing work on device-free human sensing systems to launch adversarial sensing attacks*? To answer this question, and to better understand how these attacks in the context of prior work, we review in detail existing works in device-free human sensing.

The task of "device-free human sensing" makes no assumptions on whether targets are carrying networked devices. Sensing is generally achieved by capturing and analyzing RF signals reflected off or blocked by human bodies. To be clear, this is quite different from the task of "device localization," in which the target is a networked device that communicates and synchronizes with the sensing system, *i.e.* sending and/or receiving signals (*e.g.*, [69], [33], [74], [16], [21]).

Existing works on device-free human sensing can be categorized into two broad groups: *active mode* and *passive mode*.

Active sensing. Most of the existing works fall into this group, where the sensing device continuously transmits RF signals towards the target area (Figure 1a). As some signals get reflected off the target body, they are captured by the sensing device to infer the target status (*e.g.*, [14], [13], [63], [71]). To facilitate sensing/inference, the RF signals are often custom-designed to capture information of the target, *e.g.*, frequency-modulated continuous wave (FMCW) signal [14], [13] that largely differs from WiFi transmissions. We note that some prior works on active sensing (*e.g.*, [26], [47], [73]) are branded as "passive sensing" to refer to device-free human sensing, although their sensing device is actively transmitting signals.

When considering our adversarial scenario in the context of active sensing, the key property is "detectability." Since the attacker device must *continuously* transmit RF signals, it is easy to detect, localize and remove these devices.

Passive sensing. In a passive mode, sensing devices only listen to existing transmission signals, but do not transmit signals themselves. They have no control of the RF signal used for sensing. The state-of-the-art design [63] deploys multiple sniffers to listen to WiFi signals sent by multiple transmitters in the target area, and uses these signals to detect and estimate user location. Specifically, when a user blocks the

direct line of sight (LoS) path from a transmitter to a sniffer, the original signal will diffuse around the user. By building a precise propagation model on signal diffusion on the LoS path, [63] is able to derive the user location. However, doing so requires precise location of the transmitters (cm-level). Such requirement is impractical under our adversarial scenario.

Similarly, an earlier work [17] detects the presence of a user when she disturbs the direct path between a WiFi access point (AP) and a sniffer. Again, the attacker must obtain AP locations a priori, and must deploy multiple sniffers around the target area to detect user presence (see Figure 1b).

Key observation. While some existing human sensing systems can be turned into attacks, they impose a hefty cost and risk for the attacker, significantly limiting the applicability of the attack. This motivates us to consider a new, passive human sensing attack that can be launched by a minimally equipped attacker and remains undetectable. Along these lines, our proposed attack only requires a single commodity WiFi receiver (with a single antenna) outside of the target area (Figure 1c). As we will explain in §IV, this is made possible by building a new model to detect motion using dynamics of multipath signal propagation from each anchor to the sniffer, rather than those of the direct path as in [63], [17].

III. Attack Scenario and Adversarial Model

We start by describing the attack scenario, the adversarial model, and the type of signals captured by the attacker sniffer.

Attack scenario: one sniffer and many anchors. As shown in Figure 1c, our attack leverages the ubiquity of commodity WiFi devices, ranging from routers, desktops, printers, to IoT devices like voice assistants, security cameras, and smart appliances. These devices are often spread over each room of our homes and offices [11], [10], and generally flood the surroundings with periodic WiFi packets. We refer to these WiFi devices as *anchors* in our attack.

Our attack also leverages the fact that WiFi signals are designed for significant coverage and can penetrate most walls. Thus an attacker can place a sniffer outside the target property to passively listen to existing signals sent by anchors, without compromising them or the network. Because WiFi protocols do not encrypt source and destination MAC addresses, the sniffer can isolate packets sent by each anchor, even under MAC randomization [51], [56], [41].

Our attack is effective if the sniffer can capture signals from at least one anchor per room of interest. The actual number of sniffers required depends on the size and shape of the target property and wall materials. Across all of our experiments with 11 office buildings, residential apartments and single family houses (described later in §V-B), a single sniffer is sufficient to cover our target scene.

Our attack does not work when WiFi signals do not leak to outside of the property, *e.g.* when the property has thick, concrete exterior walls. The attacker can detect this (and walk away) when either the sniffer sees too little WiFi signals, or the detected anchors are outside of the target area (§V-B).

Adversarial model. We make the following assumptions about the adversary.

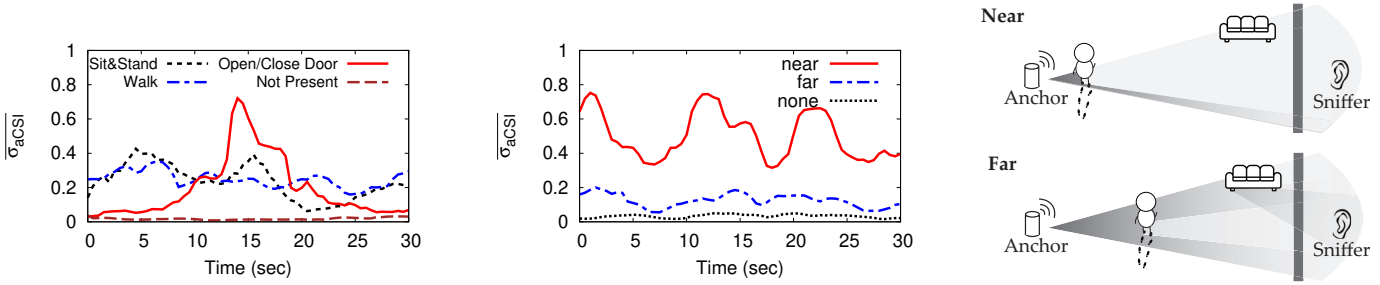
- The adversary makes no assumptions about the number, location, or movement speed of human targets being tracked.
- The adversary does not have physical or remote access to WiFi devices in the target property, or the property itself.
- Similar to the evil maid attack [2], the attacker can physically move *outside* the target property, either outside exterior walls or along public corridors, without attracting suspicion. This temporary access is necessary only for initial bootstrapping the attack, and not required for the prolonged sensing phase.
- To avoid detection, the attacker only performs passive WiFi sniffing, and avoids using any bulky or specialized hardware, *e.g.* directional antennas, antenna arrays, or USRP radios [8]. Instead, they use commodity mobile or IoT devices, *e.g.* smartphones or smart street lights. The sniffer device only needs a single (built-in) antenna.
  Note that while some smartphones (including the ones used in our attack implementation) have multiple antennas, their firmware only exposes aggregate signal received across multiple antennas, effectively giving the same amount of information as devices with a single antenna.
- The adversary partitions the target property into "regions" or virtual rooms around the anchors to detect user presence. When the adversary has access to rough floor plans of the target property[2], the attacker detects user presence down to their individual rooms.

We intentionally choose a resource-limited attacker to demonstrate the generality of this attack. Lower resource requirements imply that the attack can be successful in a wider range of practical scenarios.

Signals captured by the sniffer. For each anchor x, the sniffer S can extract two metrics from x's raw WiFi signals (even if the packets are encrypted). The first is *amplitude of channel state information (aCSI)* that measures the received signal strength (RSS) on each of the many frequency subcarriers used in a transmission. Since human movements change the multipath signal propagation from x to S, x's aCSI values seen by S will fluctuate over time. The second one is RSS, or the aggregated aCSIs over all the subcarriers. This aggregation makes RSS relatively insensitive to human movements.

A passive sniffer with a single antenna is *unable* to extract advanced signal features including phase of CSI (fCSI), Angle of Arrival (AoA) and Time of Flight (ToF) [29], [47]. Tracking fCSI and ToF requires the sniffer to actively synchronize with the transmitter [62], and estimating AoA requires the sniffer to have an antenna array [69], [30]. As mentioned earlier, while some smartphones are equipped with multiple antennas, their firmware only reports a single effective CSI but not per-antenna CSI values. Furthermore, AoA estimation requires antennas to be separated by half a wavelength (12.5cm for WiFi). Thus a reasonable array of 4 antennas will be at least 19cm in width. These physical limitations rule out the feasibility of using phase, ToF and AoA in our sensing design.

[2]Rough floor plan can often be derived from publicly available data, such as real estate websites and apps, and public building documents.



(a) $\overline{\sigma_{aCSI}}$ captures user movement

(b) $\overline{\sigma_{aCSI}}$ when the user is near, far from the anchor, or completely absent

(c) Illustration of $\overline{\sigma_{aCSI}}$'s near-far phenomenon

Fig. 2. Observations on how human movements affect an anchor's $\overline{\sigma_{aCSI}}$ seen by the sniffer. (a) $\overline{\sigma_{aCSI}}$ w/ and w/o user presence; (b)-(c) When a user moves near an anchor x, some signal paths from x to the sniffer are more frequently affected, so $\overline{\sigma_{aCSI}}(x)$ rises. As she moves away from x and has less impact on the signal propagation, $\overline{\sigma_{aCSI}}$ reduces.

IV. Turning WiFi Devices into Motion Sensors

Our attack is driven by a new aCSI variance model that links human motion near any anchor to temporal dynamics of the anchor's multipath signal propagation seen by the attacker sniffer. Whenever an anchor transmits WiFi signals, it unknowingly turns into a motion sensor for our attack. These "motion signals" are immediately seen by the attacker sniffer, who then pinpoints the targets down to their exact room(s).

Unlike prior work on passive RF sensing [63], [17], our new model focuses on capturing temporal dynamics of multipath signal propagation[3] from each anchor to the sniffer, rather than only the direct path. This lets the attacker detect any motion *around* each anchor that disturbs the multipath signal propagation, and also eliminates the need to obtain precise anchor locations and deploy multiple sniffers [63], [17].

In the following, we describe the basic observations that motivate us to pursue the attack, the key challenges it faces, and the key design concepts that make the attack feasible.

A. Correlation between Signal Dynamics and User Movement

(i) User movement → aCSI variance. In an office/home, human users are never completely stationary. Whether it is playing games, walking, opening doors, sitting down, their natural movements will disturb the multipath signal propagation of nearby WiFi transmitters (*i.e.* anchors), creating immediate, temporal variations in their aCSI values seen by the sniffer.

We propose to capture such temporal variation by a new *aCSI variance* metric:

$$\overline{\sigma_{aCSI}} = \frac{1}{|I_q|} \sum_{i \in I_q} \sigma_{aCSI}(f_i) \qquad (1)$$

where $\sigma_{aCSI}(f_i)$ represents the aCSI *standard deviation* for subcarrier i (at frequency f_i) calculated by the sniffer over a short time window (*e.g.*, 5s). We also take efforts to reduce the impact of noise and artifacts in aCSI reports by the firmware, first denoising aCSI per subcarrier using the wavelet method [75], then removing outliers by only including subcarriers whose $\sigma_{aCSI}(\cdot)$ sequences are highly correlated. The set of subcarriers used in the above calculation (I_q) are the top 50% of most correlated pairs.

Figure 2a plots several 30-second samples of an anchor's $\overline{\sigma_{aCSI}}$ seen by the sniffer, for scenarios of no human presence, a nearby user sitting down and standing up, opening/closing the door, and walking. Compared to no human presence, user movements lead to much higher $\overline{\sigma_{aCSI}}$.

We also find that user motion differs from equipment motion commonly seen in homes and offices, *e.g.* an oscillating fan and a robot vacuum. The latter either is too weak to produce any notable impact on $\overline{\sigma_{aCSI}}$ or generates periodic signal patterns different from those of human motion (§VII).

(ii) $\overline{\sigma_{aCSI}}$ depends on user-anchor distance. Another key observation is that when a target is far away from an anchor x, its movements will produce less disturbance to the signal propagation from x to the sniffer. This is demonstrated in Figure 2b, which compares an anchor x's $\overline{\sigma_{aCSI}}$ when a human user (walking) is close to x, far from x (in a different room), or completely absent.

We think this is due to the fact that a target is "bigger" when it is closer (Figure 2c). As a target moves in the space between an anchor x and the sniffer, it blocks and diffracts some signal paths from x to the sniffer. When close to x, it affects more paths than when it is far away from x. Thus the received signals seen by the sniffer will display a larger temporal variation when the user is closer to x. This phenomenon can be modeled using an abstract, ray-tracing model on $\overline{\sigma_{aCSI}}$ (omitted due to space limits). Given a fixed time period, user movements near x create more path dynamics than those far from x, leading to a larger standard deviation in the received signal strength (per subcarrier).

We validate this observation by measuring $\overline{\sigma_{aCSI}}$ of multiple anchors (Table III) in 11 test scenes (Table II). As a target moves in the space between an anchor and the sniffer, we see a general tendency of $\overline{\sigma_{aCSI}}$ decreasing with the anchor-to-target distance. We experiment with different wall materials (*e.g.*, glass, wood), distance of anchor and sniffer (8m–15m), and sniffer placement (*e.g.*, on the floor, in the bush, underneath a plastic trash can), and observe the same trend.

(iii) $\overline{\sigma_{aCSI}}$ is a more robust motion indicator than $aCSI$. Prior work [63] localizes targets by modeling $aCSI$ of the direct path. This requires an accurate propagation model and

[3]WiFi signals sent by an anchor, when arriving at the sniffer, will go through rich multipath propagation, *e.g.*, reflections by furniture, walls and human.

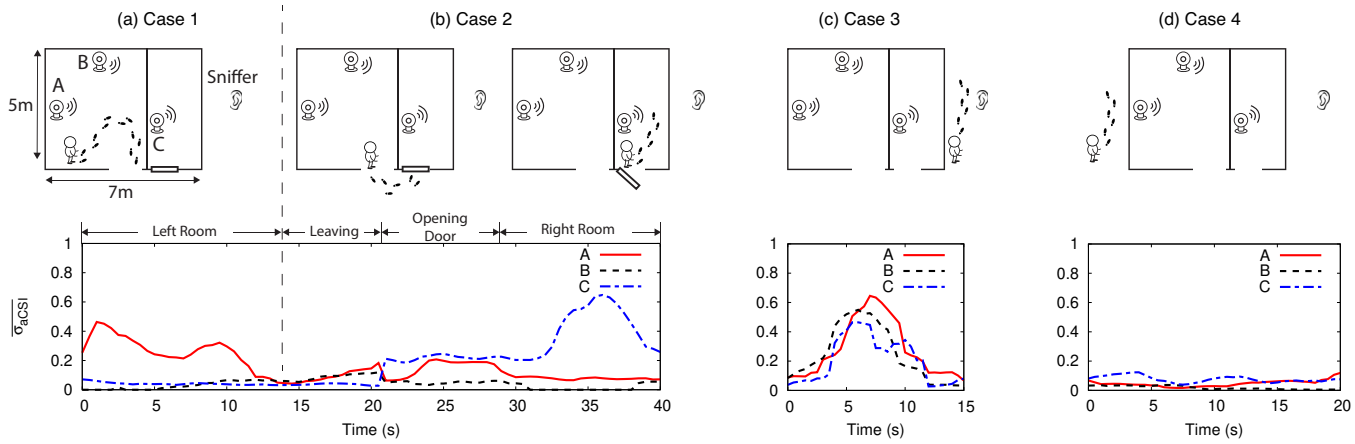


Fig. 3. Four (simple) cases on user presence and the corresponding $\{\overline{\sigma_{aCSI}}\}$ traces from anchors A, B, and C.

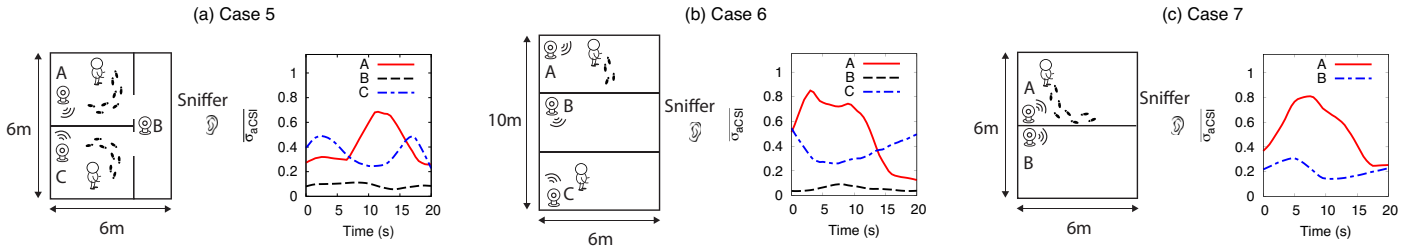


Fig. 4. Three (complex) cases on user presence and the corresponding $\{\overline{\sigma_{aCSI}}\}$ traces.

the precise physical location of each anchor. Instead, our $\overline{\sigma_{aCSI}}$ based method targets multipath dynamics caused by user motion, thus only requires knowing the room each anchor resides, rather than its precise location inside the room.

B. Challenge: Sensing Ambiguity

The above discussion suggests that with a sufficient number of anchors in a room, the sniffer should be able to detect human motion in the room from its anchors' $\overline{\sigma_{aCSI}}$. For example, if any anchor's $\overline{\sigma_{aCSI}}$ is sufficiently large, *i.e.* motion detected, the room should be marked as occupied.

But we also find notable ambiguity in such design, caused by two factors. *First*, $\overline{\sigma_{aCSI}}$ depends on the target-anchor distance and the motion pattern/strength. Yet the attacker has no knowledge of target behaviors or previous ground truth. *Second*, short physical distance to an anchor does not always translate into being the same room.

Next, we illustrate the problem of sensing ambiguity using real-world examples, including four basic cases with a single user and three complex cases with multiple users.

Case 1: Target staying in a room. Figure 3a shows the traces of $\overline{\sigma_{aCSI}}$ for three anchors: A and B in the left room, and C in the right room. The target user stays inside the left room and moves around anchor A. In this case, anchors B and C show no sign of targets nearby (very low $\overline{\sigma_{aCSI}}$) while anchor A has the largest $\overline{\sigma_{aCSI}}$ over time.

Case 2: Target moving across rooms. Following case 1, the target walks towards the room door (already open) at $t = 12s$, enters hallway at $t = 18s$, starts to open the right room door at $t = 24s$, closes it and enters the room at $t = 28s$. In this case, anchor A's $\overline{\sigma_{aCSI}}$ drops as the target moves away, followed by a short, minor increase due to the opening/closing of the right room door. Anchor C has a short, minor increase in its $\overline{\sigma_{aCSI}}$ due to the door opening/closing, followed by a significant increase as the target moves closer. Interestingly, as the target transitions between the two rooms, we can observe somewhat synchronized changes on anchor A and C (since they are triggered by the same event). But from per-anchor $\overline{\sigma_{aCSI}}$ traces, a naive design will mark both rooms as occupied.

Case 3: Sniffer blocked by external pedestrian. Pedestrians who move outside of the target area near the attack sniffer could also create aCSI variations. Yet such movements (near the common receiver) will create synchronized aCSI variations at all the transmitting anchors, regardless of any human presence. Again a naive design will mark both rooms as occupied.

Case 4: External users walking around the house. When pedestrians move away from the sniffer, the impact on $\overline{\sigma_{aCSI}}$ is small even when they are close to the anchors (Figure 3d). This is because those movements have little impact on the multi-path propagation between the anchors (inside the two rooms) and the sniffer.

Case 5: Multiple users moving in neighboring rooms. Figure 4a shows an example where two targets are moving in two different rooms, each with an anchor device. In this case, both anchors (A and C) display large $\overline{\sigma_{aCSI}}$.

Case 6: Multiple users moving in distant rooms. A user walks around in room A when another user sits down near an anchor in room C (Figure 4b). We see that room A and C's

anchors are triggered, but not the one in room B.

Case 7: Anchors on both sides of a wall. Figure 4c shows that when the user moves near anchor A, it triggers both anchor A and B (on the other side of wall). Here the simple design will mark both rooms as occupied (since both anchors are triggered), creating a false positive.

C. Design Concepts

Our analysis shows that instantaneous $\overline{\sigma_{aCSI}}$ observed at each individual anchor is insufficient to detect and localize user motion. We propose to overcome sensing ambiguity by analyzing the value and pattern of $\overline{\sigma_{aCSI}}$ across both time and anchors. The end result is a robust $\overline{\sigma_{aCSI}}$ model that links each human motion with signal dynamics of anchors in its actual room. Next, we outline the signal analysis process in two steps: 1) *detecting human motion* and 2) *mapping each motion to a room*. The detailed procedures are described later in §V-A.

Detecting human motion. If the number of detected anchors per room is reasonable[4], any user movement should "trigger" at least one anchor in the scene. But *how do we determine threshold $\sigma_p(x)$ necessary to trigger an anchor x*? This is not easy, because the adversarial has no ground truth on target presence. Also the threshold should be anchor-specific and could also vary over time.

Leveraging a common observation where a user will not stay and move in a single room forever, we propose to derive $\sigma_p(x)$ by finding "outliers." Assuming for anchor x the sniffer can measure $\overline{\sigma_{aCSI}}(x)$ over a long period of time (*e.g.*, hours or even days), it is reasonable to assume that x is mostly not triggered. Thus the sniffer can apply outlier detection methods like MAD [25], [50] to derive $\sigma_p(x)$ and adapt it over time.

Mapping Each Motion to a Room When multiple anchors in more than one room are triggered, the sniffer needs to decide whether they are triggered by users in one room (one source) or users in multiple rooms (multiple sources). This is because a target's movement could trigger anchors in neighboring rooms (case 7), and the same holds when multiple users move in two rooms (case 5 and 6). The sniffer needs to distinguish between them and determine the set of rooms that are actually occupied.

Again we leverage a common observation: human movements in different rooms are generally asynchronous, thus anchors triggered by separate sources will display different temporal patterns in $\overline{\sigma_{aCSI}}$ (case 5 and 6). But when a single source triggers anchors in neighboring rooms (case 7), these anchors' $\overline{\sigma_{aCSI}}$ will share a similar pattern. By computing the correlation of normalized $\overline{\sigma_{aCSI}}$ time series across anchors, we can determine whether they are triggered by sources in one room *i.e.* positively correlated. For example, the correlation between the two triggered anchors are -0.07, -0.03, and 0.32, in case 5, 6, and 7, respectively, and 0.23 during the door opening in case 2.

Our attack can also use the floor plan (or room transition probabilities) to fine-tune the detection result (similar to [61]). For example, a user cannot "fly" from one room to another when the rooms are widely separated. If the sniffer observes two anchors in two widely separated rooms being triggered sequentially with little or no gap, it will report two users, one in each room, rather than a single user moving across rooms.

For other cases, our attack conservatively treats the rooms with at least one anchor triggered as occupied.

[4]Home/office WiFi devices naturally spread out in a room [10], [11]. One can assume 3-4 devices in a room of common size of $25m^2$.

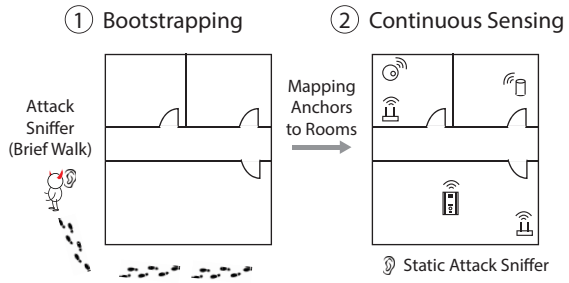


Fig. 5. Our attack process includes a bootstrapping phase and a continuous sensing phase.

V. Attack Design

After presenting the key concepts, we now present the attack design in detail. As shown in Figure 5, the attack includes two phases: (1) identify and locate anchors during "bootstrapping," and (2) deploy the sniffer and perform "continuous human sensing."

(1) Bootstrapping. The attacker first needs to identify and locate the anchors in the target area. The unique feature of our motion detection is that is does not require precise location of anchors, only their individual room. In our attack, this is achieved by the attacker performing a brief passive WiFi measurement (using the sniffer) while walking outside the target property. Similar to the evil maid attack [2], the walking measurements are only necessary during initial bootstrapping.

Before feeding the collected measurements into a device localization algorithm, our attack introduces a novel *data sifting* procedure to identify the right measurement instances for anchor localization. As a result, the attacker can localize anchors down to their individual rooms using limited and often noisy signal measurements[5].

(2) Continuous human sensing. After locating a list of anchors, the attacker hides the same sniffer at a fixed location outside the target area. The sniffer continuously monitors ambient WiFi signals, and uses them to locate and track human presence and movements inside. The sniffer also monitors each detected anchor, and any relocation of an anchor will trigger its removal from the anchor list, and possibly another *bootstrapping* phase to (re)locate the anchors.

Our proposed attack process is fully automated, and does not require any operations by the adversary, beyond the initial bootstrapping which involves a walk around the property to collect signal measurements. Note that this walking measurement could also be achieved by a robot/drone.

[5]Because the attacker has little control on the available walking path and the propagation environment, the signal measurements will inevitably contain bias, noise and human errors.

A. Continuous Human Sensing

In this phase, the sniffer will continuously collect $\overline{\sigma_{aCSI}}$ for each anchor and analyze them to detect, locate human presence to their individual rooms.

Detecting the presence of human motion. For each anchor x, when $\overline{\sigma_{aCSI}}(x) > \sigma_p(x)$, the sniffer declares the presence of motion near x, or "anchor x is triggered." To compute $\sigma_p(x)$, the sniffer applies median absolute deviation (MAD) [25], [50] on observed $\overline{\sigma_{aCSI}}(x)$ over time. Assuming "untriggered" $\overline{\sigma_{aCSI}}(x)$ follows a Gaussian distribution, we have

$$\sigma_p(x) = \lambda \cdot \text{MAD}(Z) + \text{median}(Z) \quad (2)$$

where λ is the conservativeness factor and Z is the long-term observation of $\overline{\sigma_{aCSI}}(x)$. The choice of λ will affect the motion detection rate and false alarm rate. For our attack, we set $\lambda = 11$ so the ideal detection rate per anchor is high.

Assigning target(s) to rooms. When any anchor(s) get triggered, the sniffer analyzes their temporal $\overline{\sigma_{aCSI}}$ traces to determine the set of rooms that are actually occupied.

(i) If all the triggered anchors are in the same room, then the room is declared as occupied. Exit.

(ii) If most of the anchors are triggered, and their $\overline{\sigma_{aCSI}}$ time series are (consistently) positively correlated, then the sniffer is blocked by an external pedestrian next to the sniffer, and the sensing output is "uncertain." Exit.

(iii) Now consider all the triggered anchors. Start from the triggered anchor x with the highest $\overline{\sigma_{aCSI}}$. Mark x as "checked" and its room as occupied. Compute pair-wise correlation between x and any triggered anchor (y) in neighboring rooms. If x and y are highly positively correlated, mark y as checked. Repeat until all the triggered anchors are "checked".

Tracking targets. After detecting a set of motion events, the sniffer can potentially combine them with room transition probabilities built from the floor plan to estimate user trajectories. For example, the sniffer can track a security guard's patrol route from a sequence of detected motion events.

It should be noted that while our attack can detect whether a room is occupied or not, it cannot identify an individual out of a group of users in the same room. Thus accurate per-person tracking is **only** feasible when the number of users is small.

Monitoring anchor status. The sniffer also monitors each (static) anchor's RSS (see §V-B). Upon detecting a considerable RSS change for an anchor (which indicates potential relocation), the attacker either removes it from the anchor list or run bootstrapping to relocate anchors and recompute its σ_p.

Impact of sniffer placement. The sniffer should be placed where it can capture aCSI signals from the detected anchors, while avoiding being too close to the anchors or at busy places with pedestrians frequently passing by. While one could further optimize the sniffer location, our current design randomly chooses a location that can capture signals from all the anchors.

B. Bootstrapping: Locating Anchors

During bootstrapping, the attacker uses the passive sniffer to identify and localize *static* anchors inside the target property. There are many device localization proposals, but since the sniffer stays passive and only has a single antenna, we choose to use RSS-based method [36], [38]. In this case, with a brief walk outside of the target's home/office, the adversary uses the sniffer to measure RSS of potential anchors along the trajectory. These spatial RSS values and the trajectory (recorded by the smartphone's IMU sensors) are fed into a log distance path loss model [55] to estimate the transmitter location. Each transmitter located inside the target scene area is added to the anchor list.

Why RSS but not aCSI? The localization uses RSS rather than aCSI, fCSI or AoA [58], [30] because of two reasons. *First*, our attacker sniffer only has one antenna, and cannot estimate fCSI accurately due to lack of synchronization with the transmitter. Recent work [30] estimates AoA from aCSI, but only if the sniffer has an antenna array and is in complete LoS to the targets, *i.e.* no wall. *Second*, as shown in §V-A, aCSI is sensitive to nearby target movements. As the adversary has no knowledge of the target status during bootstrapping, it cannot rely on aCSI for localization. In comparison, RSS is much more robust against target movements, thus a reliable input for localization under the adversarial scenario.

Identifying static anchors. RSS of a static transmitter, when captured by a static sniffer, should stay relatively stable, while those of moving ones will fluctuate over time. Thus before running spatial RSS measurements, the attacker will keep the sniffer static and measure the per-device RSS standard deviation (σ_{RSS}) for a period of time (*e.g.* 60s). Devices with large σ_{RSS} (>2.7dB in our work) are not used as anchors. This is repeated during the continuous sensing phase (see §V-A) to detect relocation of any anchor device. A complementary method is to infer the device type (and brand name) from the Organizational Unique Identifier (OUI) field of the MAC address [51] and ignore moveable devices like smartphones, wearables, laptops, and camera robots.

Finding high-quality RSS measurements. The localization accuracy depends heavily on the "quality" of RSS measurements. Instead of searching for a new localization design, we apply a statistical data sifting algorithm to identify proper RSS data samples as input to the localization algorithm.

The attacker can filter out "bad" measurements using denoising methods, *e.g.*, Kalman filter [20], wavelet filter [60] and feature clustering [38]. We find that these are insufficient under our attack scenarios because the propagation environment is highly complex and unknown to the adversary, making it hard to distinguish between noise and natural propagation effect. Similarly, features used by [38] to identify bad measurement rounds are too coarse-grained to effectively control localization accuracy. In fact, our experiments in §VII show that with [38], $> 50\%$ of the good measurement rounds it identifies all locate the device to a wrong room.

Instead, we propose *consistency-based data sifting* to identify proper data samples that will be used for model fitting. Our hypothesis is that, by the law of large numbers [54], *consistent* fitting results from many random samplings of RSS measurements, if exist, can reveal true signal propagation behaviors and produce high-fidelity localization results.

Given a round of measurements $\mathbb{R}$, we apply the Monte Carlo method [4] to randomly sample a subset (80%) of $\mathbb{R}$ as

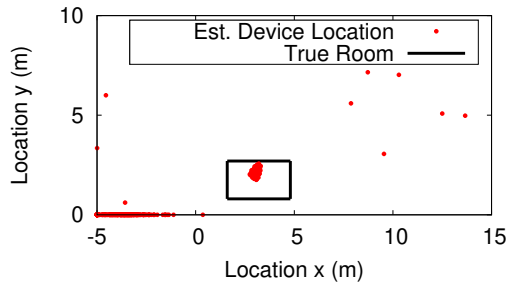


Fig. 6. Improving accuracy of anchor localization using our proposed consistency-based data sifting. Each red dot is the anchor location estimated from a Monte Carlo sample of RSS measurements. The rectangle marks the actual room the anchor resides. In this example, a dominant cluster is present and is used to estimate the final anchor location.

the input to the model fitting. This is repeated by $N = 1000$ times, producing N localization results. We can find natural clusters among these N results from their locations and fitting mean square errors (MSE). If they form many small clusters with different room placements, then $\mathbb{R}$ is inconsistent and cannot be used for localization. If a dominant cluster exists and its averaged MSE is less than those of the other clusters, then $\mathbb{R}$ can be used for localization. An example is shown in Figure 6, which produces a single, dominant cluster, while the rest are widely scattered. When such a dominant cluster is present, we can estimate the anchor room location by aggregating the location data points of the cluster. In the example of Figure 6, all the data points are located in the top center of a single room. When the data points belong to different rooms, we choose the room with the most data points.

When multiple rounds of RSS measurements are available, the attacker can apply consistency check – if a localization result is consistent across multiple rounds, then it is a confident result. Across our experiments, we find that consistency check across 4 rounds of measurements is sufficient to achieve a room placement accuracy of 92.6%.

Floor-level signal isolation. When the target property has multiple floors, the attacker needs to localize wireless anchors to a particular floor during bootstrapping. This is easily achieved using coarse angle of arrival (AoA) estimates captured by the smartphone with a simple cone cover to focus signals from a particular AoA. The received RSS from each anchor can be combined with the phone angle (via the built-in gyroscope) to localize each anchor to a floor.

VI. Smartphone Implementation

We prototype our attacker system using a commodity smartphone as the sniffer. We implement the bootstrapping and continuous sensing modules each as an Android app, and deploy and experiment using two versions of Android phones, Nexus 5 and Nexus 6. Both smartphones are equipped with the Broadcom WiFi chipset. For spatial RSS measurements (during bootstrapping), we use the built-in IMU sensors (accelerometer and gyroscope) to detect user strides and build trajectory. The key system parameters are listed in Table I.

Enabling continuous, passive sniffing of aCSI. Previously, aCSI can only be captured when the receiver actively communicates with the target transmitter [24]. Recent work [52] produces a firmware (Nexmon) that enables passive[6] sniffing, but only on a single customized transmitter at very low rates.

Parameters	Value
MAD conservative factor λ	11
Threshold of σ_{RSS} for static anchors	2.7
Ratio of Monte Carlo sampling size	80%
Number of Monte Carlo sampling rounds (N)	1000

TABLE I. Attack parameters used in our experiments.

Sniffer Path	Test Scene	# of Rooms	Mean Room Size (m^2)
Indoor Hallway	1	6	14.19
	2	7	14.60
	3	8	13.65
	4	3	14.50
	5	3	9.51
	6	6	14.21
	7	5	16.75
	8	4	44.39
	9	2	69.83
Outdoor Sidewalk	10	2	47.20
	11	4	12.99

TABLE II. Test scene configuration.

For our attack, we made a series of changes to the Nexmon firmware, so that the sniffer can run continuous passive sniffing and capture aCSI from multiple commodity WiFi devices simultaneously. In particular, we made changes to hardware buffer management to resolve the issue of buffer overflow facing the original Nexmon firmware.

One remaining artifact is that the firmware only reports aCSI at a limited speed, up to 8–11 packets per second. To save energy, we subsample sniffed packets based on this rate limit. Despite this artifact, our prototype sniffer is able to capture sufficient aCSI samples to successfully launch the attack.

Computation and energy cost. One strength of our attack is its simplicity. For our current smartphone prototype, the bootstrapping app runs 1000 rounds of Monte Carlo sampling and model fitting, which finishes in less than 25s per anchor. It takes less than 1s to compute average aCSI standard deviation. The app consumes 4.18 watts (bootstrapping) and 2.1 watts (continuous sensing), respectively. For Nexus 5 (with a built-in 2300mAh battery), this enables 4.1 hours of continuous sensing. Currently our app does not optimize for energy efficiency, which could be improved to extend sensing duration.

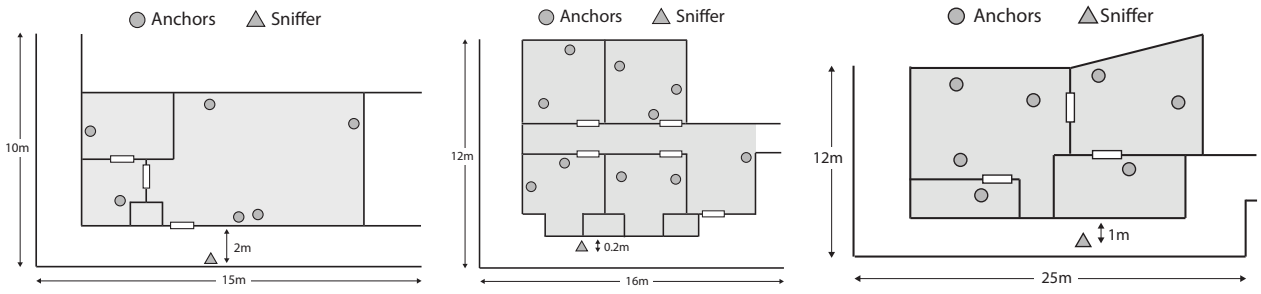
VII. Evaluation

We evaluate our attack using experiments in typical office buildings and apartments. We describe our experiment setup and test scenes, present our evaluation on individual attack phases (bootstrapping and continuous sensing), followed by an end-to-end attack evaluation.

A. Experiment Setup

We experiment at 11 typical offices and apartments that are accessible to us. The owners of each test volunteered for our experiments. The test scenes are of different sizes and configurations, and have different wall materials. The

[6]Passive sniffing means that the sniffer does not need to communicate with the target transmitter, thus remains completely undetectable.



(a) Scene 4 (b) Scene 6 (c) Scene 8

Fig. 7. Sample test scene floorplans, derived from the real estate websites or emergency exit maps, where shaded regions are the target property. We also show an instance of anchor placements where ◯s are the anchor devices, and △ is the static attack sniffer.

	Device Type	Exact Product	Mean Packet Per Second (pps), Idle	Mean Packet Per Second, Active
Static	Cameras (w/o Motion Detection)	AHD Security Camera	N/A	124
	Cameras (w/ Motion Detection)	Amcrest/Xiaomi IP Camera	$\geq$0.5	108
	Home Voice Assistance	Amazon Echo, Google Home	2	16
	Smart TV (& Sticks)	Chromecast, Apple TV, Roku	6.64	200
	Smart Switches	LifeSmart Plug	$\geq$2.44	$\geq$3.33
	WiFi Router	Xiaomi/Cisco/Asus Routers	28.6	257
Mobile	Surveillance Robot	iPATROL Riley Robot Camera	N/A	124
	Smartphones	Samsung/Google/Apple Phones	$\geq$0.5	$\geq$6

TABLE III. SUMMARY OF WIFI DEVICES USED IN OUR EXPERIMENTS. NOTE THAT OUR ATTACK WILL DETECT AND RECOGNIZE STATIC ANCHORS AND ONLY USE THEM TO DETECT/LOCALIZE HUMAN MOTION.

walking path available to the adversary also differs across experiments, from indoor corridors outside the apartment to outdoor pathways. Table II lists the test scene configuration while Figure 7 shows floor plan examples derived from publicly available data. Across all experiments, attack parameters remain unchanged (as listed in Table I).

Inside each test scene, we either reuse existing WiFi devices or deploy our own WiFi devices to emulate smart homes and offices. We use popular commodity products for smart offices and homes, *e.g.*, wireless security cameras, voice assistants, WiFi routers, and smart switches. In total, we have 31 WiFi devices, including 6 security cameras. These devices are naturally placed at locations where they are designed to be: security cameras at room corners, smart switches on the wall outlets, and WiFi routers in the center of the room for coverage. Our experiments use the 2.4GHz WiFi band due to its dominant coverage. We also test 5GHz WiFi and do not observe notable difference except its shorter coverage.

Table III summarizes these devices and their traffic patterns during idle and active periods. The packet rate varies from 0.5 packet per second (pps) to more than 100 pps. Even when idle, they still periodically transmit packets. It should be noted that to prevent attackers from inferring user presence by simply counting the packet rate of a device (if an Amazon Echo is sending more packets, it means that a human user is around), devices like home voice assistants, smart TVs, and motion-triggered cameras will need to send cover traffic when in idle state and the corresponding idle packet rate will be much higher than the listed number.

Bootstrapping. To benchmark our bootstrapping design, we collect, for each test scene, 50 walking measurements, each of 25–50 meters in length and 0.5–2 minutes in time. We also change anchor placements and repeat the experiments. In total, we collect more than 3000 RSS measurement traces, with more than 121,000 location-RSS tuples.

Continuous sensing. We place a static sniffer behind plants or at the corners (on the ground) outside of the target building within $2m$ to the building wall. We ask volunteers to carry out normal activities in each test scene and collect more than 41hrs of aCSI entries (7.8hrs of human presence, labeled). The volunteers are aware of the attack goals but not the techniques.

B. Evaluation of Continuous Human Sensing

We start from evaluating the *continuous sensing* component of our attack. Here we assume that the attacker knows the actual room where each anchor resides. By default, the attacker only uses anchors whose packet rate $\geq$ 11pps.

Performance metrics. Our goal is to evaluate whether the continuous sensing component is able to correctly detect user presence/motion in each room. We divide time into 5s slots, and run continuous sensing to estimate room occupancy in each slot based on aCSI variance values. We compare these estimates to ground truth values, and compute the detection rate and false positive rate as follows.

- *Detection rate* (DR) measures the probability of the attack reporting a room as being occupied when it is actually occupied, across all the slots.
- *False positive rate* (FP) measures the probability of a room not being occupied when our attack reports that it is being occupied.

Under our adversarial scenario, having a high detection rate is more important since the attacker does not want to miss the presence of any targets.

		# of WiFi Devices Per Room			
		1	2	3	4
Ours	DR	86.824%	95.034%	99.854%	99.988%
	FP	2.927%	4.082%	5.305%	6.935%
LiFS	DR	20.536%	37.040%	50.262%	60.821%
	FP	4.622%	4.961%	5.395%	5.886%
LiFS (unrealistic)	DR	43.568%	68.315%	82.289%	90.149%
	FP	4.622%	5.364%	6.443%	7.644%

TABLE IV. DETECTION RATE (DR) AND FALSE POSITIVE RATE (FP) OF CONTINUOUSLY HUMAN SENSING, ASSUMING ACCURATE ROOM PLACEMENT OF ANCHORS. WE COMPARE OUR DESIGN TO THE STATE-OF-ART HUMAN SENSING SYSTEM (LIFS).

Human sensing accuracy. Table IV lists the detection rate and false positive rate when we vary the number of anchors per room. We see that the detection rate scales with the number of anchors per room, reaching 86.8%, 95.03% 99.85%, and 99.988% with 1, 2, 3, and 4 anchors per room, respectively. This trend is as expected since having more anchors increases the chance that a user movement triggers at least one anchor. Furthermore, the false positive rate is low (<3%) with a single anchor per room and increases slightly to 6.9% if the attacker wants to leverage all 4 anchors. Across our experiments, the false positives mainly come from the impulse noises in aCSI reported by the firmware. Thus having more anchors will lead to more false positives.

We also compare our system to the current state of the art of passive human sensing (LiFS [63]). For fair comparison, we add wavelet denoising to LiFS, confirming that it improves the sensing performance. Since LiFS requires each anchor's precise physical location in the room (which is not available to our attacker), we first use the room center as the input to LiFS, mapping to 1–2m localization error. LiFS also requires knowledge of the aCSI value when no user is present, which we use the same MAD based method to estimate. Results in Table IV show that even with four anchors in the room, LiFS can only achieve a detection rate of 60.82%. Here the miss-detection happens when LiFS locates the human presence to a wrong room. We also run another version of LiFS that is unrealistic under our attack scenario, where each anchor's physical location error is random but bounded by 50cm (and without any room placement error). In this case, its detection rate improves, but is still far from our attack, especially with smaller number of anchors per room.

Tracking responsiveness. We also examine whether our attack is able to track human movements in time. We start from an example scenario where a user moves back and forth between two connecting rooms, *i.e.* she walks in one direction for 18s, turns around and walks in the opposite direction, and repeats. Figure 8 shows the detected user occupancy of the two rooms (each with two anchors). We see that our detection is highly responsive to rapid human movements.

We also consider all the aCSI traces collected across our test scenes and examine the duration of individual movement events estimated by the attacker. We compare these estimations to the ground truth. Figure 9 plots the cumulative distribution function (CDF) of the duration estimation error, where for 80% of the cases, the error is less than 16 seconds.

Impact of anchor packet rate. So far, our results assume

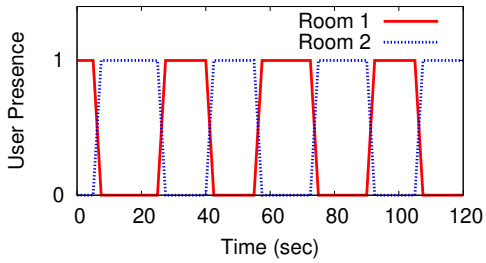


Fig. 8. The attack sniffer can track fast user motion between rooms.

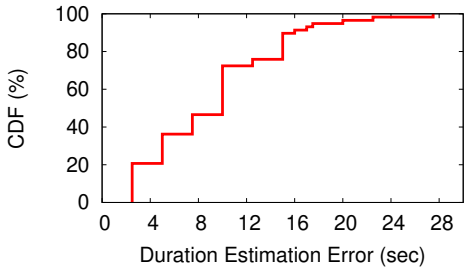


Fig. 9. Error in motion duration estimation is small.

that anchors send packets at no less than 11pps[7]. To study the impact of anchor packet rate, we take the aCSI traces of WiFi security cameras (w/o motion detection) and sub-sample them to produce desired packet rates. Our experiments show that for a single anchor per room, the detection rate is 86.824% at its full rate (an equivalent aCSI rate of 11pps), and reduces to 85.49% at 2pps, and 69.29% at 1pps. The false positive rate remains <5%. This means that each low-rate anchor can still "help" the attacker identify and locate targets. For a room with multiple low-rate anchors, the attacker will take the *union* of their detection results.

Impact of interference. During all experiments, we observe minimal impact on attack performance from interference by other WiFi transmissions out of our control or access. In the presence of strong interference, anchor packet rates will drop (due to CSMA contention) and thus human detection rate will drop as discussed earlier.

Non-human sources of motion. Smart homes and offices often have equipment that create motion even in the absence of human users. One relevant question of interest is whether these machines will be detected by the attack as human movement, leading to false positives? We experiment with a set of moving devices commonly seen in homes and offices, as well as pets, *e.g.* cats and dogs (see Table V). For example, robotic vacuums are placed on the ground level and thus have minimal impact on the sniffed signals. The only device to affect $\overline{\sigma_{aCSI}}$ in our tests is an oscillating fan. Yet its motion is highly periodic and consistent, making it easy to distinguish as non-human. We note that certain cats and dogs can also affect $\overline{\sigma_{aCSI}}$ with their movement, and their movement patterns can be hard to distinguish from human motion. Overall, our experiments show that the attack can eliminate all non-human sources of motion, except for pets.

C. Evaluation of Bootstrapping

We evaluate the bootstrapping phase (where the attacker detects and locates anchors) via two metrics: *absolute localiza-*

[7] As discussed in §VI, the sniffer's firmware reports CSI in an equivalent packet rate of 8–11pps.

Motion source	Impact on $\overline{\sigma_{aCSI}}$	Distinguishable from human motion?
Server internal cooling fan	No	-
Standing fan	No	-
Oscillating fan	Yes	Yes
Robot vacuum	No*	No
Cats or dogs	Yes	No

TABLE V. IMPACT OF SOURCES OF NON-HUMAN MOTION ON OUR ATTACK. (*) A ROBOT VACUUM ONLY AFFECTS $\overline{\sigma_{aCSI}}$ OF AN ANCHOR IN CLOSE PROXIMITY WHEN THE ANCHOR IS PLACED ON THE FLOOR.

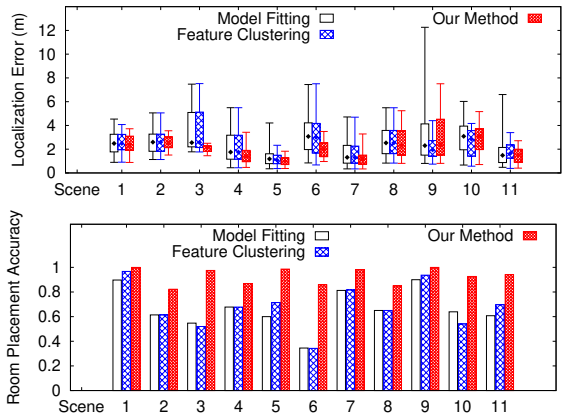


Fig. 10. Bootstrapping performance: anchor localization accuracy in terms of absolute localization error (m) and room placement accuracy, per test scene.

tion error which is the physical distance between the ground-truth location and the attacker-estimated location, and *room placement accuracy* which is the probability of placing an anchor to its exact room. Figure 10 plots, for each test scene, the quantile distribution of the absolute localization error and the room placement accuracy. We compare three systems: the model-fitting algorithm that uses all the measurements, the feature-clustering based data filtering proposed by [38], and our consistency-based data sifting method.

Gain of consistency-based data sifting. The results show that our proposed data sifting method can largely improve anchor localization accuracy compared to the two existing approaches. Our method largely reduces the localization error tail, and for more than 90% of the cases, the attacker places the anchor at the right room. Our method outperforms [38] by using fine grained, scene-specific features to filter data.

An interesting observation is that in scene 8–10, our method faces a similar (and even larger) absolute localization error than feature clustering but produces higher room placement accuracy. This is because our design directly analyzes the consistency of room placements, rather than raw localization errors. Smaller raw localization error does not always translate into higher room placement accuracy.

Impact of anchor placements. As expected, it is relatively harder to accurately locate anchors placed at room boundaries, *e.g.*, those plugged into wall outlets. In many cases, these boundary anchors create a dominant Monte Carlo cluster, but the data points in the cluster map to either of the two neighboring rooms. Our current design simply chooses the room with more data points, which could lead to room placement errors.

When the number of anchors is sufficiently large, the attacker can minimize the impact of such boundary anchors in two ways. First, the attacker can either use these boundary anchors "with caution" or not use them at all. Second, the attacker can leverage past human sensing results to discovery any strong correlation between anchors and adjust their room placements. We leave these to future work.

		# of WiFi Devices Per Room			
		1	2	3	4
Ours	DR	80.603%	94.210%	98.780%	99.725%
	FP	3.595%	5.962%	8.386%	10.719%
LiFS	DR	14.153%	26.381%	36.954%	46.033%
	FP	14.024%	14.077%	14.493%	15.064%

TABLE VI. END-TO-END PERFORMANCE OF OUR ATTACK VS. LIFS, IN TERMS OF DETECTION RATE (DR) AND FALSE POSITIVE RATE (FP).

Impact of anchor packet rate. The accuracy of our proposed anchor localization method is relatively insensitive to anchor packet rate. This is likely because RSS (of static anchors) is relatively stable over time. As long as the measurement trace covers >20m in distance and the RSS values are between -75dB and -30dB without strong bias, we observe little difference in localization (and room placement) accuracy.

D. End-to-End Attack Evaluation

Finally, we evaluate the end-to-end performance of our attack, combining the bootstrapping and continuous sensing phases. Like §VII-B, we consider the detection rate and false positive rate for the task of detecting and localizing human users to their individual rooms. The results will include the impact of any misplaced anchors during bootstrapping, or errors in detecting/localizing users during continuous sensing.

Table VI lists the detection rate and false positive rate for our attack design and those achieved via LiFS [63]. We also vary the number of WiFi anchor devices in each room. Compared to the results in Table IV assuming accurate anchor room placement, the end-to-end attack sees minor drop in both recall and precision, especially with more anchors per room. Despite using a passive, minimally equipped attacker device, our attack still achieves high human sensing accuracy, *e.g.*, 99.7% detection rate at 10.71% false positive rate.

The impact of anchor localization errors is much more visible on LiFS, whose detection rate drops to 36.954% and 46.033% even with 3 and 4 anchors in each room, respectively. Overall, we see that while both using the same aCSI values per anchor, our proposed passive human sensing largely outperforms LiFS by not requiring precise anchor location to model signals on the direct propagation path.

VIII. DEFENSES

We now explore robust defenses against our proposed attack and other passive sensing attacks. Our design insight is that attack effectiveness depends heavily on the quantity and quality of the WiFi signals captured by the sniffer. Thus a defense reducing the amount of WiFi signal leakage to external sniffers or adding inconsistency to WiFi signals could render the attack ineffective.

A. MAC Randomization

The first solution coming to mind would be *MAC address randomization*, a well-known method for protecting mobile

devices against tracking. Since the attack sniffer uses MAC address to isolate signals of anchors, MAC randomization can disrupt both bootstrapping and continuous sensing phases. However, recent work has shown that MAC randomization is disabled on most devices (<3% of adoption rate so far) [42] and can be easily broken to reveal the real MAC address [41], [5]. We note that Android 9.0 Pie switches to per-network MAC randomization [7], which does not apply any MAC randomization to static WiFi devices. Thus MAC randomization is not a plausible defense against our attack.

B. Geofencing WiFi Signals

Geofencing bounds signal propagation to reduce or eliminate WiFi signals accessible to the adversary. In our attack, when the area with a signal in our walking trace reduces from 25–50 meters to 10 meters or less, the anchor localization error increases significantly: raw errors more than double, and anchor room placement accuracy drops from 92.6% to 41.15%.

Geofencing is also extremely difficult to deploy and configure. The simplest form is to reduce the anchor's transmit power, which is almost always undesirable since it degrades connectivity. Another option is to equip WiFi devices with directional antennas, limiting signal spatial coverage. This is also undesirable as it requires upgrading to equipment with higher cost and larger form factors, as well as carefully configuring antenna directionality. Finally, the extreme solution is to block RF propagating beyond property walls by painting these walls with electromagnetic shielding paints. This is again impractical, since it blocks incoming WiFi/cellular signals.

If the area accessible to the attacker is limited, a potential solution is to customize WiFi signal coverage using 3D fabricated reflectors [70] or backscatter arrays [39] that create noise towards the area. Yet both remain open research problems.

C. WiFi Rate Limiting

While geofencing reduces spatial leakage of WiFi signals, rate limiting reduces their temporal volume. When anchors transmit less signals over time, the sniffer will not have sufficient data to compute $\overline{\sigma_{aCSI}}$. Results in §VII show that reducing anchor packet rates does lower the detection rate (when using a single anchor) but can be compensated by aggregating the results of multiple anchors.

In practice, rate limiting is undesirable for most network applications. As shown in Table III, many WiFi devices, when idle, already transmit at more than 2pps. It is hard to rate limit further, rendering the defense ineffective.

D. Signal Obfuscation: Existing Designs

Signal obfuscation adds noise to WiFi signals, so the adversary cannot accurately localize anchors or detect user motion. Existing works have proposed both temporal and spatial obfuscations against RF sensing [38], [48].

In *temporal obfuscation*, WiFi devices (anchors) change transmit power randomly over time, injecting artificial noises to signals seen by the sniffer. Doing so, however, requires upgrading commodity WiFi devices to equipment with much higher cost and energy consumption. Also a more resourceful adversary can counter by deploying an extra static sniffer (during bootstrapping) to infer the injected signal power changes and remove them from the signal traces, as shown by [38].

In *spatial obfuscation*, a recent work [48] shows that by deploying a full-duplex radio near each anchor x, one can obfuscate x's signal phase, RSS, CSI, and Doppler shift seen by any nearby sniffers with a single antenna. But full-duplex radios are of high cost, and there is no commodity product on the market. On the other hand, defending against our attack only needs to obfuscate RSS and aCSI, collected by the sniffer.

E. Proposed: AP-based Signal Obfuscation

The above four immediate defenses are either ineffective or impractical. Instead, we propose a practical defense where the WiFi access point (AP) actively injects customized cover traffic for any of its associated WiFi device w that is actively transmitting. We design this defense to produce large ambiguity to the attack in two steps. *First*, our defense adds noise to the attacker's RSS measurements, so that during bootstrapping, the attacker will place most of the anchors to the wrong room and even outside of the property. *Second*, our defense largely reduces (and even removes) the $\overline{\sigma_{aCSI}}$ gap between no human presence and human motion, such that the attacker is unable to identify human motion.

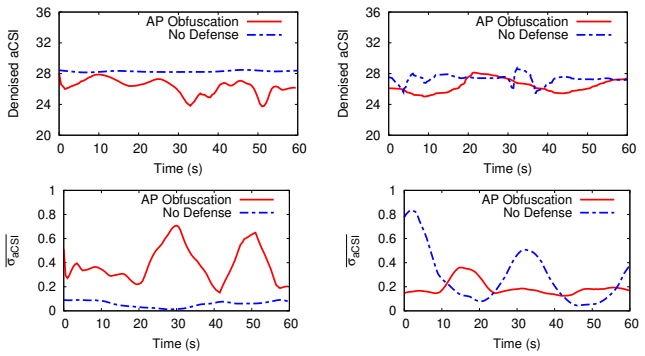
AP inserting customized cover signal. As soon as the AP detects a transmission from w, it estimates w's transmission rate T_w and injects a cover traffic stream with the rate of ρT_w, at a randomized power level and with w's MAC address. ρ is the injection rate, a system parameter. Since the AP limits its cover traffic stream to be proportional to w's throughput, the CSMA protocol will randomly interleave packets from the two streams together. In the worst case (ρT_w is at or higher than available channel throughput), the cover traffic will reduce w's effective throughput by $1 + \rho$.

The insertion of "fake" packets requires a careful design, so that it disrupts the attack rather than creating obvious "anomalies" or heavily affecting the WiFi network. In particular, the AP configures the sequence numbers of fake packets to (partially) interleaved with those of real packets, so that the attacker is unable to separate the two streams based on sequence number and packet arrival time. When sending fake packets, the AP's transmit power is randomized but close to that of w, so the mixed traffic follows natural (and complex) multipath signal variation. This makes it hard to distinguish real and fake packets from signal strength values alone.

Finally, this defense can be deployed on today's WiFi APs that support transmit power adaptation with minor changes. The major overhead is the extra consumption (a factor of ρ) of bandwidth and energy at the AP.

Results: Impact on bootstrapping. With this defense, the attacker's RSS measurements of anchor w will display fluctuations, tricking the sniffer to think that w is moving and not use it as an anchor. Even if the adversary assumes w is stationary, the noisy RSS measurements (even after our data sifting) will lead to inaccurate room placement.

When evaluating this defense, we consider both our original attacker (with one smartphone) and an *advanced* attacker who adds an extra stationary sniffer and applies RSS signal



(a) User not present (b) User in motion

Fig. 11. aCSI and $\overline{\sigma_{aCSI}}$ with and without AP based signal obfuscation.

subtraction to detect and remove any "injected" signal variations [38]. We configure our defense where the AP injects cover traffic of ρ with power randomization in the $10dB$ range. For both attackers, ρ=5% is sufficient to drop the accuracy of anchor room placement from 92.6% (without our defense) to 35.71%, except for the anchors close to the AP (in the same room). As we further increase ρ, the attacker will map most of the detected anchors to the AP's room.

Results: Impact on continuous sensing. As the attacker sniffer calculates $\overline{\sigma_{aCSI}}(w)$ on randomly interlaced packets sent by anchor w and the AP, the value of $\overline{\sigma_{aCSI}}(w)$ with no human presence will increase significantly. Figure 11(a) shows a sample trace of aCSI (of a sub-carrier) and $\overline{\sigma_{aCSI}}$ with and without the defense. We see that our defense can effectively elevate the threshold $\sigma_p(w)$ for human presence detection. More importantly, the defense has much less impact on $\overline{\sigma_{aCSI}}(w)$ when there is actual human movement near the anchor w. The sample traces in Figure 11(b) show that $\overline{\sigma_{aCSI}}(w)$ actually drops (below the threshold) when using the proposed defense. In this case, human movement will not trigger any anchor in proximity, for both the original and the advanced attackers (who deploy an extra sniffer).

Table VII lists the attack performance with our proposed defense (ρ=30%) and without any defense. We first consider the case where the attacker manages to obtain perfect anchor room placement. In this case, our defense increases the false positive rate from 7.9% to 48.28% while dropping the detection rate to 78.776%. Next, we consider the end-to-end attack scenario where the attacker performs both bootstrapping and continuous sensing. Our defense drops the detect rate down to 47.48% while increasing the false positive rate to 49.5%. These results apply to both the original attacker and the advanced attacker. Such ambiguity renders the attack useless in practice.

	False positive rate		Detection rate	
	No defense	AP obf	No defense	AP obf
knowing anchor room placement	7.935%	48.284%	99.988%	78.776%
end-to-end attack	10.719%	49.598%	99.725%	47.481%

TABLE VII. THE ATTACK PERFORMANCE UNDER AP-BASED SIGNAL OBFUSCATION (BEST PERFORMANCE OUT OF THE ORIGINAL AND THE ADVANCED ATTACK WITH AN EXTRA SNIFFER).

Possible countermeasures. To overcome our proposed defense, the attacker must find ways to distinguish the obfuscation packets sent by AP from the original packets sent by an anchor w. As discussed earlier, doing so using packet sequence number and arrival time is infeasible due to our packet injection method. Doing so at the network traffic level is also difficult, since packet contents are encrypted, and we can shape traffic to resist traffic identification by attackers [15]. Finally, it is also difficult to separate the two streams using physical layer characteristics, because doing so requires much more sophisticated and bulky hardware. One option is to analyze per-symbol aCSI/RSS patterns. This is infeasible using commodity WiFi chips, as they only report per-packet aCSI/RSS values. Another option is to use a large antenna array (MIMO with at least 4–6 antenna elements, each separated by 6.25cm) to distinguish signals sent by w from those sent by the AP, since they come from different directions. The resulting sniffer (>31cm in length) would be conspicuous and easily raise suspicion.

IX. Related Work

Human sensing by snooping signals. We categorize existing works into five groups. The first group applies *traffic analysis* to infer user presence and status in a home/office from their network traffic [35], [51], [77], [18], [49], [45], [12]. It requires strong knowledge on device behaviors and can be easily countered by sending cover traffic, applying encryptions and traffic shaping. In contrast, our attack remains effective even when all network-level defenses are deployed, as long as WiFi devices still transmit packets.

The second group uses "specialized signals" such as RFID [78], visible light [76], [37], and acoustic [40], [44], that often correlate with human motion. But existing solutions require control of transmitters inside or outside of the target property, which is infeasible under our attack model.

The third group builds *fingerprints* of each predefined target location and/or activity, based on either aCSI [43], [66], [75], CSI [46], [65], RSS [26], [59], [53], [57], or raw signals [67]. Since the attacker under our model has no knowledge of the target users and access to the target property, building fingerprints becomes infeasible.

The fourth group uses advanced radio hardware (laptops or USRPs with antenna arrays or directional antennas) that communicate with the anchors inside the target property. This allows the sniffer to measure fine-grained CSI values (both amplitude and phase) [68], and use them to calculate AoA and doppler frequency shift (DFS) to detect human motion [29], [47], [65], [72], [28], [19]. Our attack differs by using a passive sniffer with a single antenna, which does not communicate/synchronize with the anchors. In this case, the sniffer cannot infer CSI phase, AoA or DFS.

The final group detects user motion using passive sniffers to collect and analyze physical RF signals [17], [19], [63]. As discussed earlier, both [17], [63] target user motion that disturbs the direct propagation path, requiring precise locations of the anchors. [19] uses multiple sniffers with bulky directional antennas to compute doppler shift of user motion. The sensing method used by our attack falls into this category, but targets multipath signal propagation from each anchor to the sniffer. We design a new aCSI variance model to reliably detect user

motion, eliminating the need for precise anchor location and antenna array at the sniffer.

Passive transmitter localization. Existing works often leverage bulky receivers with multiple antennas [14], [33], [58], [30], [69], [34] to estimate signal AoA, and applies triangulation across receivers to derive target location. Our anchor localization (during bootstrapping) uses a compact smartphone with a single antenna, and applies passive localization that fits spatial RSS measurements to a propagation model [27], [38], [23]. Our key contribution is the data sifting algorithm that identifies good RSS samples as input to the model fitting.

Defense against RF sensing. Existing works [32], [48], [22], [64] defend against eavesdropping on a transmitter by a jammer transmitting simultaneously, preventing the attacker from decoding packets or estimating CSI/AoA. This requires precise synchronization between the transmitter and the jammer [31] or a high-cost full-duplex obfuscator [48]. Our defense uses AP to insert fake packets (rather than transmitting simultaneously), which is easy to deploy and effective against our attack.

X. Conclusion

Our work shows that the ubiquity of WiFi devices has an unexpected cost: reflected or blocked RF transmissions leak information about our location and activities. We describe a set of low-cost, stealthy reconnaissance attacks that can continuously monitor and locate human motion inside a private property, turning WiFi devices inside into motion sensors. All this is done without compromising the WiFi network, data packets or devices, and only requires a commodity WiFi sniffer outside of the property. We validate the attack on a variety of real-world locations, and develop a new effective defense based on carefully tuned WiFi signal obfuscation by APs.

We believe our work points to the potential of more powerful information leakage attacks via passive RF reflections. With more sophisticated signal processing techniques (and potentially new hardware), much more might be learned from the way ambient RF signals interact with our bodies and surroundings. We are pursuing this line of research to both better understand these attacks and to develop defenses to better safeguard our security and privacy.

Acknowledgment

We thank our shepherd Earlence Fernandes and the anonymous reviewers for their feedback. We also thank Vyas Sekar and Fadel Adib for their feedback on the early version of this work. This work is supported in part by the National Science Foundation grants CNS-1923778 and CNS-1705042. Any opinions, findings, and conclusions or recommendations expressed in this material do not necessarily reflect the views of any funding agencies.

References

[1] "About thermal imaging," https://pr-infrared.com/about-thermal-imaging/thermal-imaging-faq.

[2] "Evil maid attack," http://searchsecurity.techtarget.com/definition/evil-maid-attack.

[3] "The first 5 things to do with new smart lights," https://www.cnet.com/how-to/the-first-5-things-to-do-with-your-smart-lights/.

[4] "HOWTO estimate parameter-errors using monte carlo," http://www-personal.umd.umich.edu/~wiclarks/AstroLab/HOWTOs/NotebookStuff/MonteCarloHOWTO.html, 2014.

[5] "Researchers break MAC address randomization and track 100% of test devices," https://www.bleepingcomputer.com/news/security/researchers-break-mac-address-randomization-and-track-100-percent-of-test-devices/, 2017.

[6] https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/, 2018.

[7] "Android P feature spotlight: Per-network MAC address randomization added as experimental feature," https://www.androidpolice.com/2018/03/08/android-p-feature-spotlight-per-network-mac-address-randomization-added-experimental-feature/, 2018.

[8] "Ettus research products," https://www.ettus.com/product/, 2018.

[9] https://www.statista.com/statistics/802706/world-wlan-connected-device/, 2019.

[10] "Smart home layout," https://www.hornernetworks.com/smart-home-layout, 2019.

[11] "Smart layouts," https://onefirefly.com/creative-services/smart-layouts, 2019.

[12] A. Acar, H. Fereidooni, T. Abera, A. K. Sikder, M. Miettinen, H. Aksu, M. Conti, A. Sadeghi, and A. S. Uluagac, "Peek-a-boo: I see your smart home activities, even encrypted!" *CoRR*, vol. abs/1808.02741, 2018.

[13] F. Adib, Z. Kabelac, and D. Katabi, "Multi-person localization via RF body reflections," in *Proc. of NSDI*, 2015.

[14] F. Adib and D. Katabi, "See through walls with WiFi!" in *Proc. of SIGCOMM*, 2013.

[15] N. Apthorpe, D. Reisman, S. Sundaresan, A. Narayanan, and N. Feamster, "Spying on the smart home: Privacy attacks and defenses on encrypted iot traffic," *CoRR*, vol. abs/1708.05044, 2017.

[16] P. Bahl and V. N. Padmanabhan, "RADAR: an in-building RF-based user location and tracking system," in *Proc. of INFOCOM*, 2000.

[17] A. Banerjee, D. Maas, M. Bocca, N. Patwari, and S. Kasera, "Violating privacy through walls by passive monitoring of radio windows," in *Proc. of WiSec*, 2014.

[18] Y. Cheng, X. Ji, T. Lu, and W. Xu, "DeWiCam: Detecting hidden wireless cameras via smartphones," in *Proc. of Asia CCS*, 2018.

[19] K. Chetty, G. E. Smith, and K. Woodbridge, "Through-the-wall sensing of personnel using passive bistatic WiFi radar at standoff distances," *IEEE Transactions on Geoscience and Remote Sensing*, vol. 50, no. 4, 2012.

[20] F. Evennou and F. Marx, "Advanced integration of WiFi and inertial navigation systems for indoor mobile positioning," *EURASIP J. Appl. Signal Process*, vol. 2006, 2006.

[21] Z. Farid, R. Nordin, and M. Ismail, "Recent advances in wireless indoor localization techniques and system," *Journal of Computer Networks and Communications*, vol. 2013, 2013.

[22] S. Gollakota and D. Katabi, "iJam: Jamming oneself for secure wireless communication," Computer Science and Artificial Intelligence Laboratory Technical Report, Tech. Rep., 2010.

[23] A. Goswami, L. E. Ortiz, and S. R. Das, "WiGEM: A learning-based approach for indoor localization," in *Proc. of CoNEXT*, 2011.

[24] D. Halperin, W. Hu, A. Sheth, and D. Wetherall, "Tool release: Gathering 802.11n traces with channel state information," *ACM SIGCOMM CCR*, vol. 41, no. 1, 2011.

[25] F. R. Hampel, "The influence curve and its role in robust estimation," *Journal of the American Statistical Association*, vol. 69, no. 346, pp. 383–393, 1974.

[26] H. Huang and S. Lin, "WiDet: Wi-Fi based device-free passive person detection with deep convolutional neural networks," in *Proc. of MSWIM*, 2018.

[27] Y. Ji, S. Biaz, S. Pandey, and P. Agrawal, "ARIADNE: A dynamic indoor signal map construction and localization system," in *Proc. of MobiSys*, 2006.

[28] W. Jiang, C. Miao, F. Ma, S. Yao, Y. Wang, Y. Yuan, H. Xue, C. Song, X. Ma, D. Koutsonikolas, W. Xu, and L. Su, "Towards environment independent device free human activity recognition," in *Proc. of MobiCom*, 2018.

[29] K. Joshi, D. Bharadia, M. Kotaru, and S. Katti, "WiDeo: Fine-grained device-free motion tracing using rf backscatter," in *Proc. of NSDI*, 2015.

[30] C. R. Karanam, B. Korany, and Y. Mostofi, "Magnitude-based angle-of-arrival estimation, localization, and target tracking," in *Proc. of IPSN*, 2018.

[31] M. Khaledi, M. Khaledi, S. K. Kasera, and N. Patwari, "Preserving location privacy in radio networks using a stackelberg game framework," in *Proc. of Q2SWinet*, 2016.

[32] Y. S. Kim, P. Tague, H. Lee, and H. Kim, "Carving secure Wi-Fi zones with defensive jamming," in *Proc. of Asia CCS*, 2012.

[33] M. Kotaru, K. Joshi, D. Bharadia, and S. Katti, "SpotFi: Decimeter level localization using WiFi," in *Proc. of SIGCOMM*, 2015.

[34] M. Kotaru and S. Katti, "Position tracking for virtual reality using commodity WiFi," in *Proc. of CVPR*, 2017.

[35] H. Li, Y. He, L. Sun, X. Cheng, and J. Yu, "Side-channel information leakage of encrypted video stream in video surveillance systems," in *Proc. of INFOCOM*, 2016.

[36] L. Li, G. Shen, C. Zhao, T. Moscibroda, J.-H. Lin, and F. Zhao, "Experiencing and handling the diversity in data density and environmental locality in an indoor positioning service," in *Proc. of MobiCom*, 2014.

[37] T. Li, Q. Liu, and X. Zhou, "Practical human sensing in the light," in *Proc. of MobiSys*, 2016.

[38] Z. Li, Z. Xiao, Y. Zhu, I. Pattarachanyakul, B. Y. Zhao, and H. Zheng, "Adversarial localization against wireless cameras," in *Proc. of HotMobile*, 2018.

[39] Z. Li, Y. Xie, L. Shangguan, R. I. Zelaya, J. Gummeson, W. Hu, and K. Jamieson, "Towards programming the radio environment with large arrays of inexpensive antennas," in *Proc. of NSDI*, 2019.

[40] W. Mao, J. He, and L. Qiu, "CAT: High-precision acoustic motion tracking," in *Proc. of MobiCom*, 2016.

[41] J. Martin, T. Mayberry, C. Donahue, L. Foppe, L. Brown, C. Riggins, E. C. Rye, and D. Brown, "A study of MAC address randomization in mobile devices and when it fails," *CoRR*, vol. abs/1703.02874, 2017.

[42] C. Matte and M. Cunche, "Spread of MAC address randomization studied using locally administered mac addresses use historic," *RR-9142, Inria Grenoble Rhône-Alpes*, 2017.

[43] R. Nandakumar, B. Kellogg, and S. Gollakota, "Wi-Fi gesture recognition on existing devices," *CoRR*, vol. abs/1411.5394, 2014.

[44] R. Nandakumar, A. Takakuwa, T. Kohno, and S. Gollakota, "Covertband: Activity information leakage using music," in *Proc. of UbiComp*, 2017.

[45] T. OConnor, R. Mohamed, M. Miettinen, W. Enck, B. Reaves, and A.-R. Sadeghi, "Homesnitch: Behavior transparency and control for smart home iot devices," in *Proc. of WiSec*, 2019.

[46] Q. Pu, S. Gupta, S. Gollakota, and S. Patel, "Whole-home gesture recognition using wireless signals," in *Proc. of MobiCom*, 2013.

[47] K. Qian, C. Wu, Y. Zhang, G. Zhang, Z. Yang, and Y. Liu, "Widar2.0: Passive human tracking with a single Wi-Fi link," in *Proc. of MobiSys*, 2018.

[48] Y. Qiao, O. Zhang, W. Zhou, K. Srinivasan, and A. Arora, "PhyCloak: Obfuscating sensing from communication signals," in *Proc. of NSDI*, 2016.

[49] S. V. Radhakrishnan, A. S. Uluagac, and R. Beyah, "GTID: A technique for physical device and device type fingerprinting," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 5, 2015.

[50] P. J. Rousseeuw and C. Croux, "Alternatives to the median absolute deviation," *Journal of the American Statistical association*, vol. 88, no. 424, pp. 1273–1283, 1993.

[51] I. Sanchez, R. Satta, I. N. Fovino, G. Baldini, G. Steri, D. Shaw, and A. Ciardulli, "Privacy leakages in smart home wireless technologies," in *Proc. of ICCST*, 2014.

[52] M. Schulz, J. Link, F. Gringoli, and M. Hollick, "Shadow Wi-Fi: Teaching smart- phones to transmit raw signals and to extract channel state information to implement practical covert channels over Wi-Fi," in *Proc. of MobiSys*, 2018.

[53] M. Seifeldin, A. Saeed, A. E. Kosba, A. El-Keyi, and M. Youssef, "Nuzzer: A large-scale device-free passive localization system for wireless environments," *IEEE Transactions on Mobile Computing*, vol. 12, no. 7, 2013.

[54] P. K. Sen and J. M. Singer, Eds., *Large sample methods in statistics*. Chapman & Hall, Inc., 1989.

[55] J. Seybold, *Introduction to RF Propagation*. Wiley, 2005.

[56] S. Siby, R. R. Maiti, and N. O. Tippenhauer, "IoTScanner: Detecting privacy threats in iot neighborhoods," in *Proc. of IoTPTS*, 2017.

[57] S. Sigg, M. Scholz, S. Shi, Y. Ji, and M. Beigl, "RF-Sensing of activities from non-cooperative subjects in device-free recognition systems using ambient and local signals," *IEEE Transactions on Mobile Computing*, vol. 13, no. 4, 2014.

[58] E. Soltanaghaei, A. Kalyanaraman, and K. Whitehouse, "Multipath triangulation: Decimeter-level WiFi localization and orientation with a single unaided receiver," in *Proc. of MobiSys*, 2018.

[59] V. Srinivasan, J. Stankovic, and K. Whitehouse, "Protecting your daily in-home activity information from a wireless snooping attack," in *Proc. of UbiComp*, 2008.

[60] S. Tan and J. Yang, "WiFinger: Leveraging commodity WiFi for fine-grained finger gesture recognition," in *Proc. of MobiHoc*, 2016.

[61] D. Vasisht, A. Jain, C.-Y. Hsu, Z. Kabelac, and D. Katabi, "Duet: Estimating user position and identity in smart homes using intermittent and incomplete RF-data," in *Proc. of UbiComp*, 2018.

[62] D. Vasisht, S. Kumar, and D. Katabi, "Decimeter-level localization with a single WiFi access point," in *Proc. of NSDI*, 2016.

[63] J. Wang, H. Jiang, J. Xiong, K. Jamieson, X. Chen, D. Fang, and B. Xie, "LiFS: Low human-effort, device-free localization with fine-grained subcarrier information," in *Proc. of MobiCom*, 2016.

[64] T. Wang, Y. Liu, Q. Pei, and T. Hou, "Location-restricted services access control leveraging pinpoint waveforming," in *Proc. of CCS*, 2015.

[65] W. Wang, A. X. Liu, M. Shahzad, K. Ling, and S. Lu, "Understanding and modeling of WiFi signal based human activity recognition," in *Proc. of MobiCom*, 2015.

[66] Y. Wang, J. Liu, Y. Chen, M. Gruteser, J. Yang, and H. Liu, "E-eyes: Device-free location-oriented activity identification using fine-grained WiFi signatures," in *Proc. of MobiCom*, 2014.

[67] N. Xiao, P. Yang, Y. Yan, H. Zhou, and X. Li, "Motion-Fi: Recognizing and counting repetitive motions with passive wireless backscattering," in *Proc. of INFOCOMM*, 2018.

[68] T. Xin, B. Guo, Z. Wang, M. Li, Z. Yu, and X. Zhou, "Freesense: Indoor human identification with wi-fi signals," in *Proc. of GLOBECOM*, 2016.

[69] J. Xiong and K. Jamieson, "ArrayTrack: A fine-grained indoor location system," in *Proc. of NSDI*, 2013.

[70] X. Xiong, J. Chan, E. Yu, N. Kumari, A. A. Sani, C. Zheng, and X. Zhou, "Customizing indoor wireless coverage via 3D-fabricated reflectors," in *Proc. of BuildSys*, 2017.

[71] L. Yang, Y. Chen, X.-Y. Li, C. Xiao, M. Li, and Y. Liu, "Tagoram: Real-time tracking of mobile RFID tags to high precision using cots devices," in *Proc. of MobiCom*, 2014.

[72] S. Yousefi, H. Narui, S. Dayal, S. Ermon, and S. Valaee, "A survey on behavior recognition using WiFi channel state information," *IEEE Communications Magazine*, vol. 55, 2017.

[73] M. Youssef, M. Mah, and A. Agrawala, "Challenges: device-free passive localization for wireless environments," in *Proc. of MobiCom*, 2007.

[74] M. Youssef, A. Youssef, C. Rieger, U. Shankar, and A. Agrawala, "PinPoint: An asynchronous time-based location determination system," in *Proc. of MobiSys*, 2006.

[75] H. Yu, B. Yang, J. Liu, and G. Yu, "Passive human trajectory tracking study in indoor environment with csi," in *Proc. of NaNA*, 2018.

[76] C. Zhang and X. Zhang, "LiTell: Robust indoor localization using unmodified light fixtures," in *Proc. of MobiCom*, 2016.

[77] F. Zhang, W. He, X. Liu, and P. G. Bridges, "Inferring users' online activities through traffic analysis," in *Proc. of WiSec*, 2011.

[78] J. Zhang, G. Tian, A. M. J. Marindra, A. Imam, and A. Zhao, "A review of passive RFID tag antenna-based sensors and systems for structural health monitoring applications," *Sensors*, vol. 17, 2017.