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

Published NDSS (2020)
By Zhu et al.

February 2021

Outline

Background

Attack Scenario

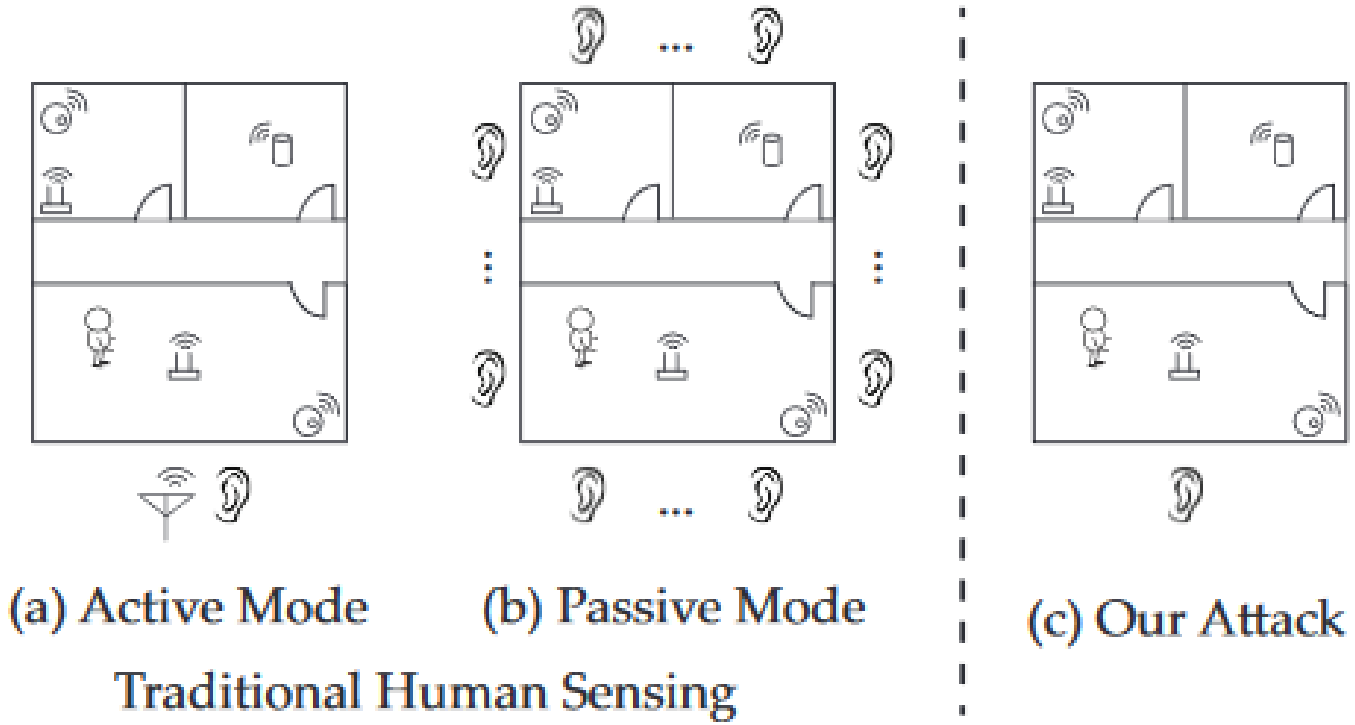
Adversarial Model

Attack Design

Evaluation

Defenses

Summary



All they use the signals to detect user location

Background Work

- **Active sensing** work (Device continuously transmits RF signals):
  - Most works appear on this area
  - Signals get reflected off the target body,
    - They are captured by the sensing device to infer the target status
  - Since the attacker device must continuously transmit signals, it is easy to detect
- **Passive sensing** work (Devices only listen and do not transmit signals):
  - Multiple sniffers that listen to WiFi signals sent by multiple transmitters in the target area
  - A mechanism to detect the presence of a user when he disturbs the direct path between a WiFi AP and a sniffer
    - The attacker must obtain AP locations a priori and deploy multiple sniffers around the target area

Motivation

- There are human sensing systems that can be turned into attacks but they impose a hefty cost and risk for the attacks
  - This limits the applicability of the attack
- Can we simply reuse existing work on device-free human sensing systems to launch adversarial sensing attacks?
- Can we find a passive human sensing attack that can be launched by a minimally equipped attacker and remain undetected?

Contribution

- A silent attack that continuously detect, monitor/locate human motion behind walls
  - Uses a novel model on multipath signal dynamics to remove dependences on active transmissions
  - Remain undetectable
  - Low cost (cheap commodity hardware). ONLY a single WiFi receiver (with a single antenna)
  - No need to compromise devices or decode/decrypt the network traffic
- The attack was validated in real-world settings.
- A practical and effective defense using AP-based obfuscation

WiFi signal propagation

- 1) User movement near a WiFi transmitter changes its signal propagation in a way that can be observed by nearby receivers
- 2) Walls and buildings today are not built insulated against WiFi signals
  - Signals sent by devices inside a property can often be overheard by outside receivers

Motion Detection via multipath signal dynamics

- The model links together
  - Human motion near WiFi transmitters
  - Variances of multipath signal propagation seen by a sniffer outside of the property
- When a human moves near a WiFi device ***x***, the motion changes the multipath signal propagation to the attacker sniffer ***S***.
  - This model allows S to capture such signal dynamics and use them to pinpoint the target to a specific location
- OF COURSE: The more WiFi devices inside the property, the more accurate tracking

Assumptions

- No knowledge about the WiFi network and the devices inside the property (including their locations)
- At least one WiFi device inside a room is needed for the attack to be effective
  - In case of relocating a sensor, the attack still works as accurate as before

Limitations

- The model is unable to identify features like: speed, activity type and user identity or separate humans from large animals.
- A passive sniffer with a single antenna cannot extract advanced signal features including phase of CSI, Time of Flight (ToF), Angle of Arrival (AoA) etc.

Attack Scenario

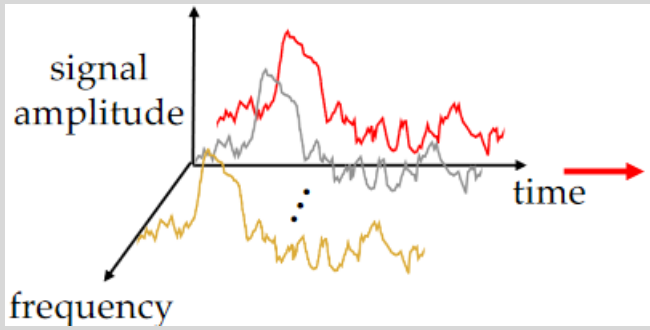
- **One sniffer and many anchors**
  - The attack leverages the ubiquity of commodity WiFi devices (e.g. routers, printers)
    - These devices are often spread over each room of a home and office
    - These WiFi devices will be referred as **anchors** in this presentation
  - The attack leverages the fact that WiFi signals are designed for significant coverage and can penetrate most walls
    - Attackers can place a sniffer outside the target property to passively listen to signals
  - Recall: WiFi protocols do not encrypt source/destination MAC addresses
    - Thus, the sniffer can isolate packets sent by each other

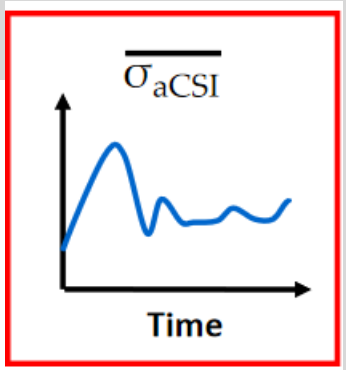
Adversarial Model

- Adversary **makes no assumptions** about the number, location or movement speed of human targets being tracked
- He **does not have physical access** to WiFi devices in the target property
- He **can physically move *outside* the target property**, either outside exterior walls or along public corridors without attracting suspicion
- To avoid detection, **he** only **performs passive WiFi sniffing**, without any specialized hardware. He needs a sniffer that has only a single built-in antenna
- He **divides the target property into "regions"** around the anchors to detect user presence.

Measuring Signal Variation via CSI

- This attack leverage the **Channel State Information (CSI)**, which captures the signal strength under different carriers
- To measure the variation, first gather the raw value of CSI
- Compute the standard deviation for each sub-frequency
- Average those standard deviations across different sub-frequencies
- Result: The average $\overline{\sigma_{aCSI}}$

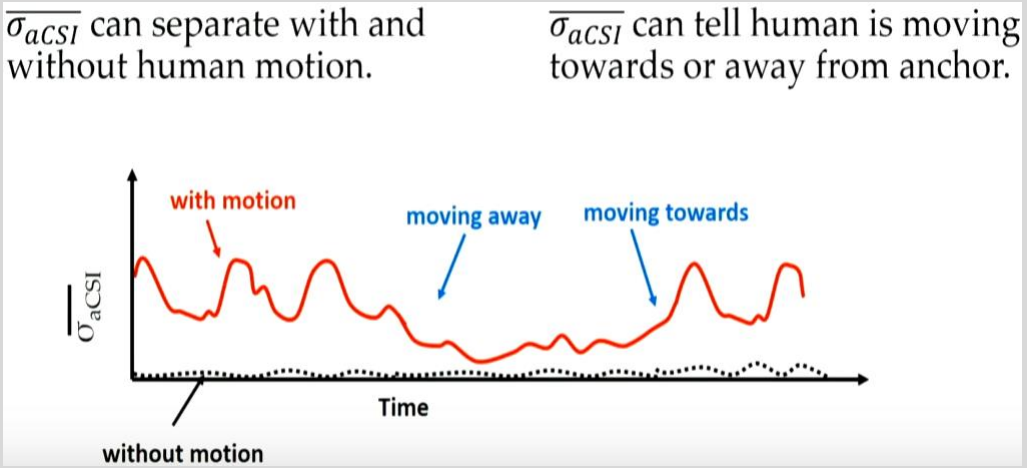




Our final metric

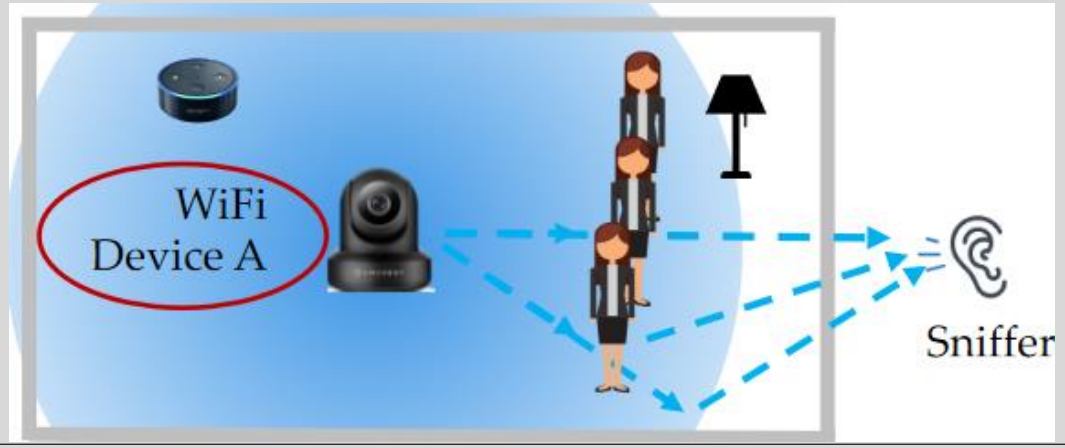
Observations (1)

- **User movement → aCSI variance**
  - Humans are never completely stationary (e.g., playing games, walking)
    - Their natural movements will disturb the multipath signal propagation of nearby WiFi transmitters (i.e. anchors), creating variations in their aCSI values seen by the sniffer

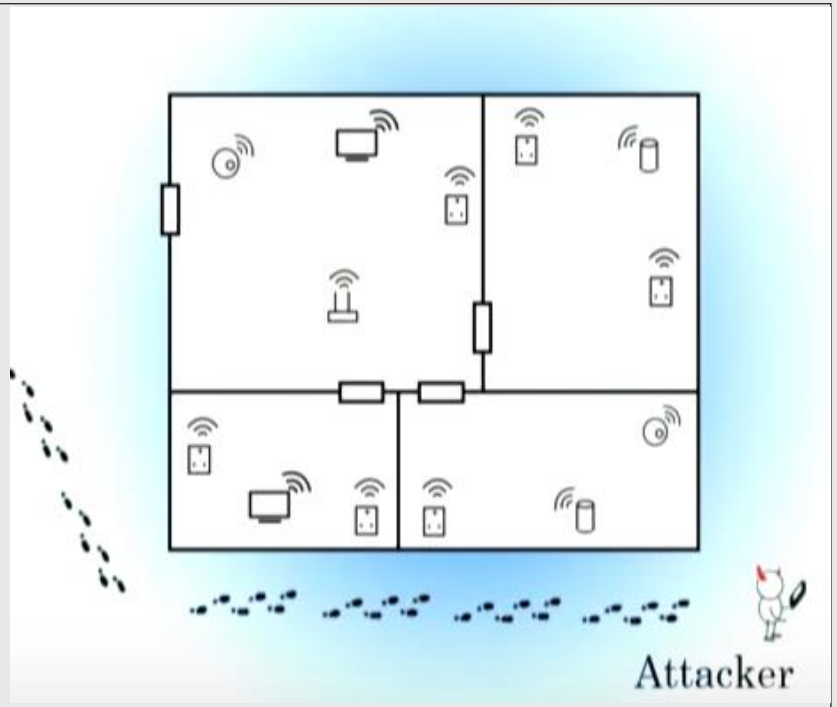


Observations (2)

- 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

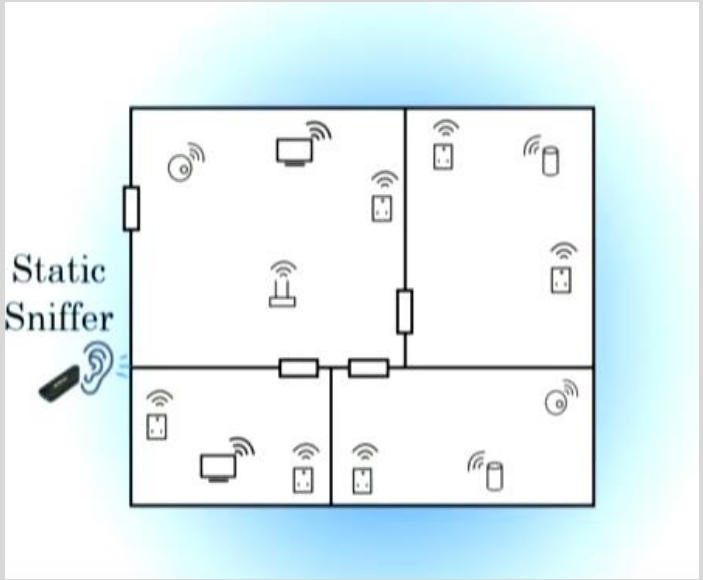


Attack Design (1)



- **Two steps:**
  - **Bootstrapping,**
  - **Continuous monitoring**
- **Identify and locate anchors during "bootstrapping"**
  - The attacker 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.
  - This is achieved by the attacker **performing** a brief **passive WiFi measurement** while walking outside the target property.

Attack Design (2)



- **Deploy the sniffer and perform "continuous human sensing."**
  - The **attacker hides the** same **sniffer** at a fixed location outside the target area.
  - The **sniffer continuously monitors WiFi signals**, and uses them to locate human presence.
  - The **sniffer monitors each detected anchor**, and any relocation of an anchor will trigger its removal from the anchor list,
    - We need another bootstrapping phase to (re)locate the anchors

Evaluation (1)

- **Experiments**
  - 11 homes & offices with various floorplans
  - 31 WiFi devices
    - These devices are naturally placed at locations where they are designed to be
  - A static sniffer outside of the target building within 2m to the target
  - Modified the WiFi firmware to passively collect CSI
  - The volunteers are aware of the attack goals but not the techniques

Evaluation (2)

- Having more anchors increases the chance that a user movement triggers at least one anchor.

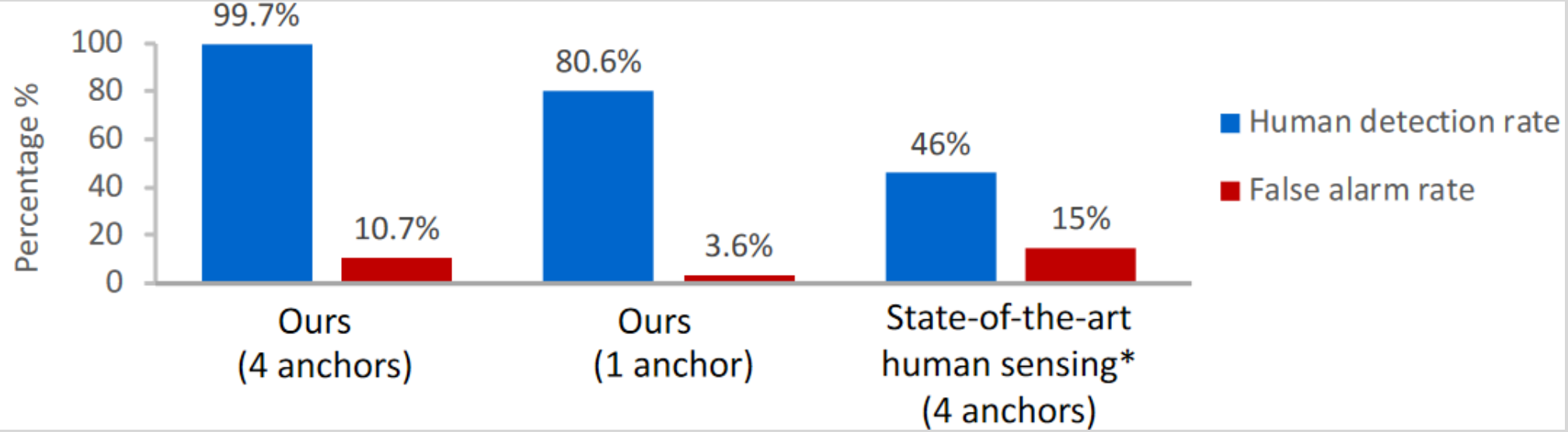
- **Detection rate(DR)** measures the probability of the attack reporting a room as being occupied when it is actually occupied, across all the slots.
- **False positive rate(FP)** measures the probability of a room not being occupied when our attack reports that it is being occupied.

$$\text{Human detection rate} = \frac{\text{T(attacker reports room has human inside)}}{\text{T(room has human inside)}}$$

$$\text{False alarm rate} = \frac{\text{T(room does not have human inside)}}{\text{T(attacker reports room has human inside)}}$$

Is the attack effective?

- **LiFS** requires each anchor's precise physical location in the room (which is not available to our attacker), we 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,



*** LiFS: Low human-effort, device-free localization with fine-grained subcarrier information. MobiCom'16.**

Is the attack robust?

- How effective is the attack at low-rate packet?
  - Human detection **drops only 1.5%** when anchors transmits at 2 packets per second, compared to full rate 11pps
- How about non-human sources motions?
  - **Human motion differs from equipment motion** commonly seen in homes (e.g.an oscillating fan and a robot vacuum).
    - The latter either is **too weak to produce any notable impact** on aCSI or generates periodic signal patterns different from those of human motion

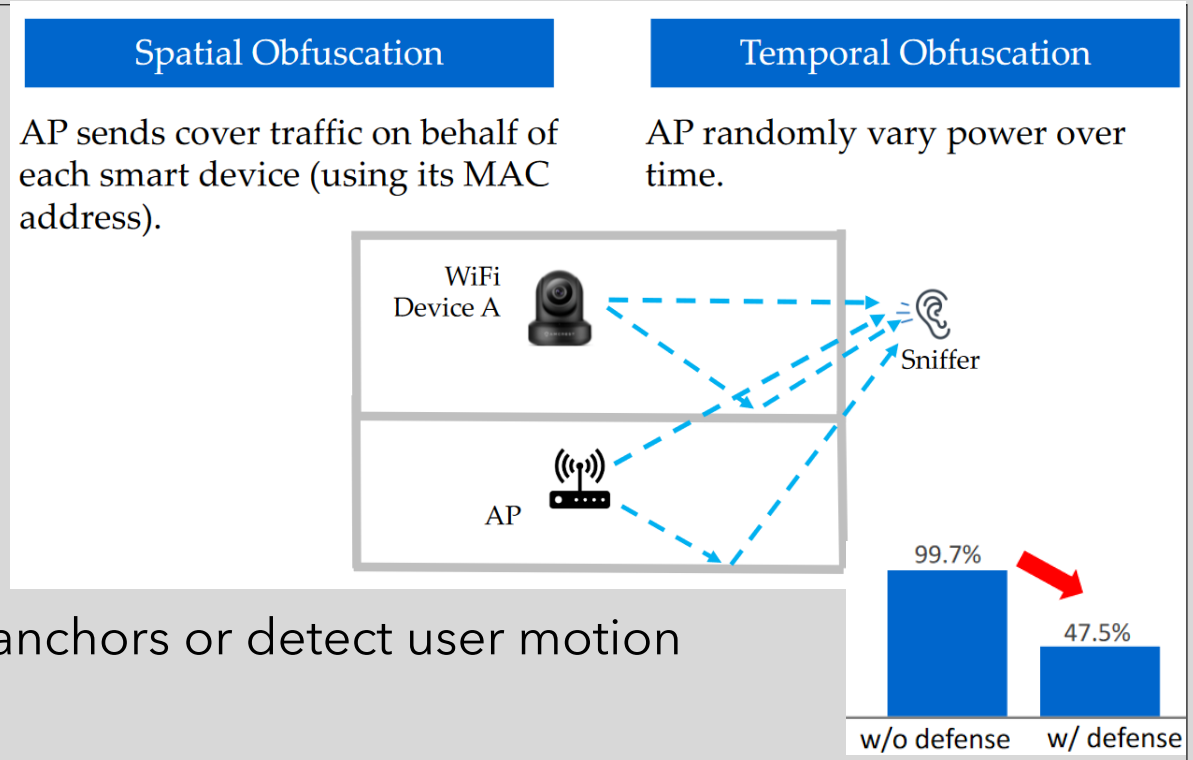
Existing Defenses (1)

- The **effectiveness of the attack depends** heavily on the **quantity** and **quality** of the WiFi signals captured by the sniffer
- **MAC Randomization**
  - Since the attack sniffer uses MAC address to isolate signals of anchors, MAC randomization can disrupt both bootstrapping and continuous sensing phases
    - This featured **is disabled on most devices** (according to recent work)
    - Android 9.0 switches to per-network MAC randomization, which does not apply any MAC randomization to static WiFi devices

Existing Defenses (2)

- **Geofencing**
  - Bounds signal propagation to reduce WiFi signals accessible to the adversary
  - Geofencing is also difficult to deploy and configure:
    - Reduce the anchor's transmit power, which is almost always undesirable since it degrades connectivity.
    - Equip WiFi devices with directional antennas, limiting signal spatial coverage.
      - Higher cost and larger form factor
- **WiFi rate limiting**
  - Is undesirable for most network applications. Many **WiFi devices, when idle, transmit at more than 2pps**. It is hard to rate limit further, rendering the defense ineffective.

Proposed Defense (1)



- **Signal obfuscation by AP**
  - Adds noise to WiFi signals
    - Adversaries cannot accurately localize anchors or detect user motion
- **Spatial obfuscation**
  - The **WiFi AP** actively **injects customized cover traffic** for any of its associated WiFi devices **w** that is actively transmitting.
    - This **produces large ambiguity** to the attack
- **Temporal obfuscation**
  - WiFi devices change transmit power randomly over time, injecting artificial noises to signals seen by the sniffer
    - It needs equipment with higher cost/energy consumption

Summary

- **An adversary can accurately detect and track movements of users**
  - **No compromisation** of any device is needed
  - **Only passive WiFi signal analysis**
- It seems to be **effective under real conditions**
- Defense:
  - **AP-based obfuscation** is quite effective

THANK YOU!

Questions?