I Always Feel Like Somebody's Sensing Me! A Framework to Detect, Identify, and Localize Clandestine Wireless Sensors

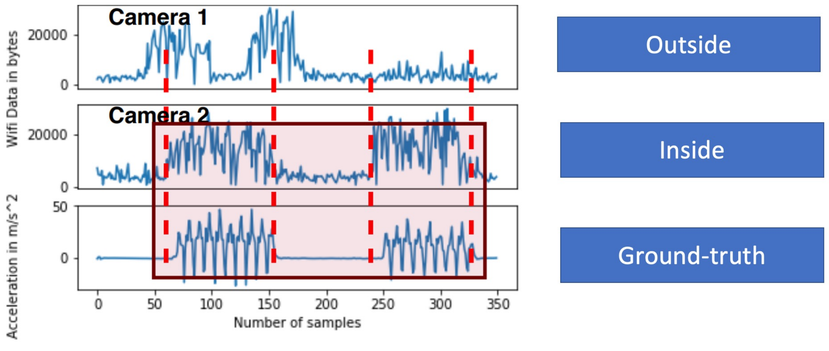
Akash Deep Singh, Luis Garcia, Joseph Noor, and Mani Srivastava (UCLA)

Objective

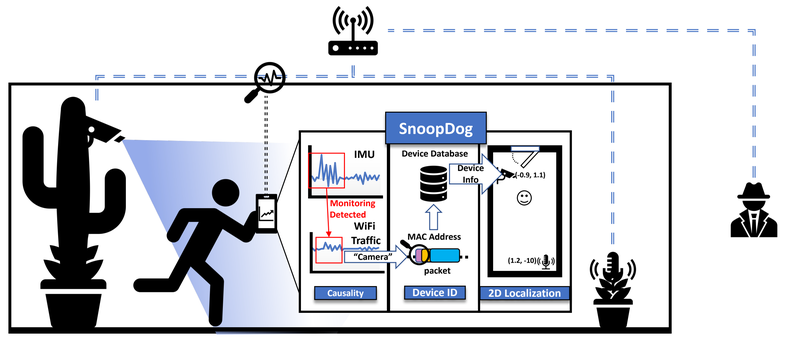
- To develop a framework that can detect, identify and localize wireless sensors that are monitoring a user in unknown, uncontrollable or adversarial spaces.

Approach: Detection

- **Hypothesis:** The traffic of a sensor monitoring a user should change in response to the actions of the user.
- Wi-Fi based sensors such as cameras, smart-home assistants and motion sensors encode their traffic using Variable Bit Rate encoding (VBR) techniques for the purposes of bandwidth and power efficiency.
- VBR techniques allow these sensors to send less information when the scene is static and more information when the scene is dynamic.
- If we have a trusted ground truth sensor (sensorA) that can measure the changes in the scene, we can use this ground truth sensor and the network traffic of the snooping sensor(sensorB) to establish a cause-effect relationship to validate our hypothesis.
- We use Wireshark to sniff the traffic of all the sensors in the space and then use Granger Causality to ascertain whether a cause-effect relationship exists between the sensorA and sensorB.
- The ground truth sensor also allows us to ignore sensors whose traffic is showing variation, but this variation is not in response to the user's actions as shown below.



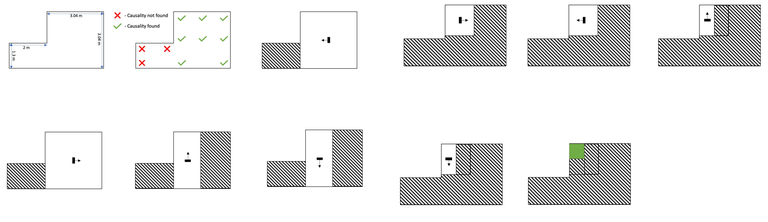
Detecting cause-effect relationship between the traffic of a camera monitoring a user (Camera 2) and a ground truth sensor (Accelerometer measuring the user's motion). Camera 1 which is not monitoring the user does not have a cause-effect relationship



Overview of SnoopDog framework. 1) The SnoopDog framework first identifies if a user is being monitored based on the cause-effect relationship between the values of a trusted sensor, e.g., an IMU, and Wi-Fi traffic patterns. It then inspects the associated packets and identifies the possible devices based on the physical (MAC) address. 2) Finally, SNOOPDOG localizes each device by leveraging directionality and sensor coverage.

Approach: Localization

- Sensors such a cameras, motion sensors as well as microphones are directional – their traffic only changes when the scene within their field-of-view (FOV) changes.
- If the change in scene is blocked by an object, or at a volume lower than what the sensor can perceive – the scene seems static to the sensor.
- This directionality can be exploited to create a 2D localization technique in which a user can first stand in the center of the room, flash colors/create some motion/play some sound while simultaneously blocking this from the other side using their body or varying the volume.
- If a camera is in front of the user, it's traffic will change while if a camera is behind the user, it will have no changes in its traffic.



Successive elimination-based trials that exploit directionality can be used to reduce the total search space iteratively as shown in the figure above.

Results

- We evaluated our framework on 13 different sensors ranging from cameras to smart-home assistants, RF sensor and motion sensors.
- In over 200 trials, SnoopDog was able to accurately detect the snooping sensor with an accuracy of ~95%.
- The mis-detections occurred when the cameras froze or when there were additional users in the scene who were also moving – which was not accounted for by the ground truth sensor.

Conclusions

- Cause-effect analysis between user's ground truth actions and the traffic of a sensor using Variable Bit Rate (VBR) encoding can help ascertain whether the sensor is spying on the user or not.
- Using directionality of sensors along with cause-effect analysis in a successive elimination manner can reveal where a sensor is placed in the scene. A user can follow this trial-based elimination method to reduce the search space sufficiently.

Path Forward

- Extend the framework to work on standards beyond Wi-Fi.
- Extend the framework to work in cases where the adversary is using evasion techniques, such as channel hopping, data padding, no encoding or MAC randomization.
- Develop methods to detect wireless devices employing Low Probability of Detection (LPD) schemes.
- Extend the current methods to opportunistically collect additional information about clandestine sensors such as their IP address, operator information and triggers.

Publications

- Singh, A. D., Garcia, L., Noor, J., & Srivastava, M. "I Always Feel Like Somebody's Sensing Me! A Framework to Detect, Identify, and Localize Clandestine Wireless Sensors." 30th {USENIX} Security Symposium ({USENIX} August). 2021

POINT OF CONTACT: Akash Deep Singh akashdeepsingh@g.ucla.edu