Inferring the Scene Using Wireless Traffics and World Knowledge

Xiaoyi Han & Binglu Chen

Motivation and Objects

- smart home IoT devices & low-cost wireless sensors
- privacy leakage

- an attack methodology
- infer human movement within a specific room
  - wireless traffic from camera sensors
  - world knowledge
- demonstrate the serious privacy threats

Technical Approach and Novelty

- RF-based Localization and Tracking → just infer position
- Wireless Signal-based Human Activity Recognition →
  - an extra device
  - a specific environment
- User Behavior Analysis in IoT Devices →
  - access sensor data like app usage history and movement patterns
  - use a set of simple sensors, whose patterns are identified

Technical Approach and Novelty

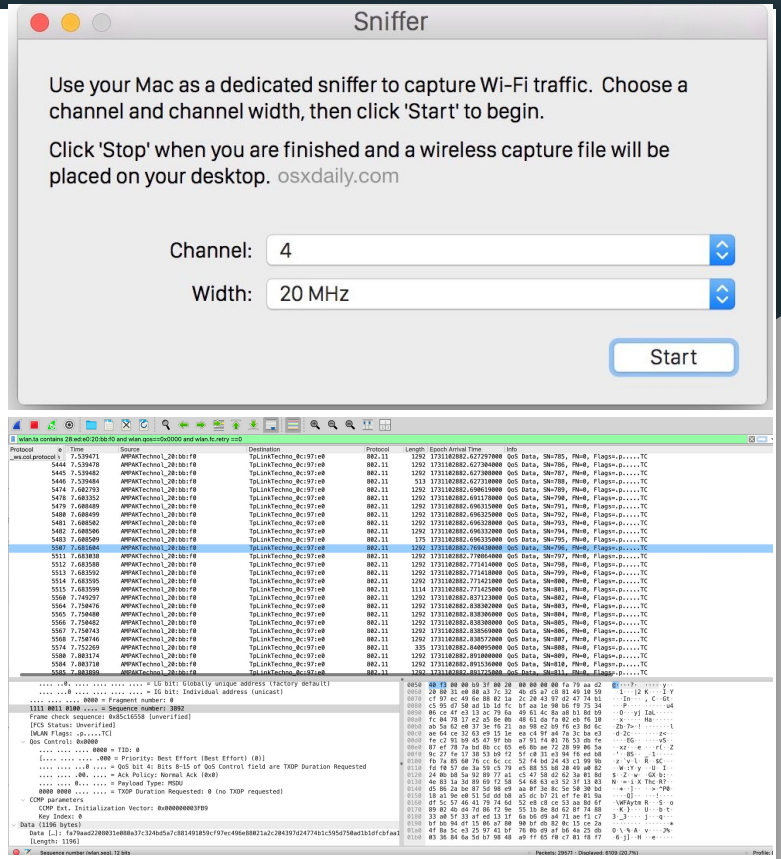
- wifi packets based
  - Use a computer to capture the wifi packets from camera and router
  - Compared to RSSI- and CSI-based methods, we don’t need a receiver
- camera transmission rule H.264
  - Camera is the most commonly used sensor in our home
  - Camera has helpful video compression tech H.264
  - The transmission rate varies depending on the video type
- requires no wifi access
  - Same as a real-world scenario, our project use the encrypted data to analyse
- using world knowledge to help identify the different scenarios

Methods

Step1: Use a MacBook Wi-Fi sniffer to capture Wi-Fi packets.

Step2: Analyze Wi-Fi traffic using Wireshark software.

Step3: Leverage a large language model (LLM) to extract features from the captured data.

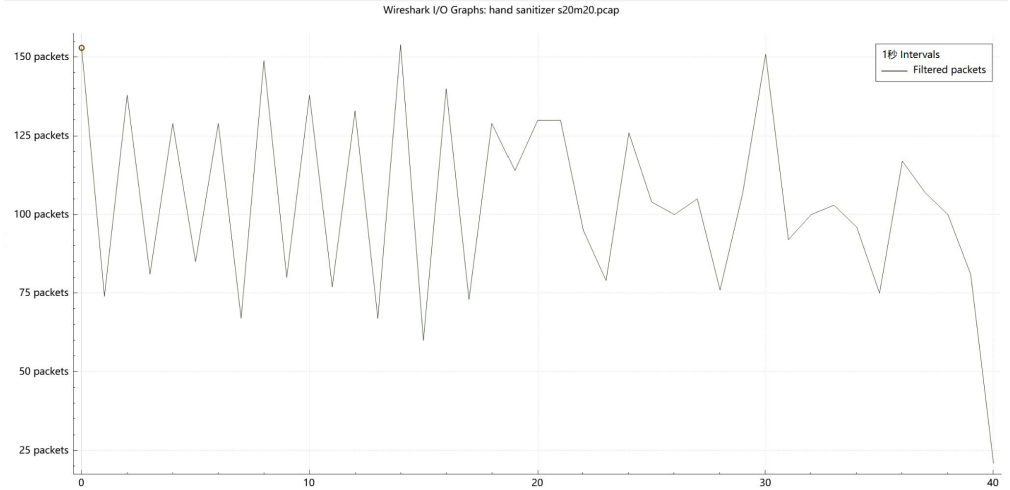


Evaluation and Metrics

- Detect Motion Changes in User Behavior
  - moving from static to active states
  - shifting from a slow pace to a faster one
  - changing from small-range movements (e.g., hand gestures) to large-range movements (e.g., walking)
- The intensity of the movement: Velocity and Range
  - Using LLM to get the targets' change of movement speed and range information
- Accuracy, Precision and Recall to evaluate the success

Current Status and Next Steps

The graph of static 20s and moving 20s



- Find the mapping between package number/length and IPB frame (H.264)
- Write code to distinguish different movement mode and to train the network

Thank you!