PoDC: WiFi spying

Seeing, keylogging and hearing through walls

papers:

See Through Walls with WiFi!
Tracking Keystrokes Using Wireless Signals
We Can Hear You with Wi-Fi!

François Wirz | 23-05-2017
Motivation: Sensing with Wireless Signals

- Coarse granularity
  - tracking position in room
Motivation: Sensing with Wireless Signals

- **Coarse granularity**
  - tracking position in room

- **Fine granularity**
  - tracking gesture through walls
  - binary H2M communication through walls
Motivation: Sensing with Wireless Signals

- **Coarse granularity**
  - tracking position in room

- **Fine granularity**
  - tracking gesture through walls
  - binary communication through walls

- **Very fine granularity**
  - tracking keystrokes
  - tracking lip movements
Technical Primer

Constructive interference

Destructive interference

image sources: all images are adapted from the respective paper, except where stated otherwise
image src: http://pediaa.com/difference-between-constructive-and-destructive-interference/
Technical Primer: Interference Nulling

Interference nulling with two sources

image src: http://pediia.com/difference-between-constructive-and-destructive-interference/

Technical Primer: Beamforming

Beamforming through constructive interference
MIMO is used in:

- WiFi 802.11n standard
- LTE standard
- Power-line communication
Technical Primer: Multiple-Input Multiple-Output

- MIMO
  - allows to focus the signal emitted (beamforming)
  - allows signal to cancel out in a plane (interference nulling)
  - can use multiple senders or multiple receivers or both
  - more uniform signal that can be amplified (no receiver saturation)

Technical Primer: Flash effect

- Flash effect
  - most of the signal gets reflected by the first obstacle
  - cancels out all weaker signal from behind
    - signal from bodies is drowned in noise
    - cannot amplify signal because receiver would saturate
Technical Primer: Flash effect

- Other approaches use larger devices:
  - 2 GHz of bandwidth (UWB)
  - strong power source
  - large antenna array (2.5 m)
Technical Primer: Inverse Synthetic Aperture

- **Synthetic Aperture Sensing**
- **Inverse Synthetic Aperture Sensing**
  - use temporal signal to extract spatial information
  - obtain angle of motion

![Diagram of Antenna Array and Angle of Arrival](image src: https://people.csail.mit.edu/fadel/papers/wivi-poster.pdf)
See Through Wall: WiVi

- Applying these techniques with WiVi:
See Through Wall: WiVi

WiVi: angle and motion
WiVi: Gesture encoding

- Standard Return-to-zero encoding
  - Encode 0 bit as step forward, step back
  - Encode 1 bit as step back, step forward
See Through Wall: WiVi

- Property used
  - MIMO interference nulling at wall, first obstacle
  - Inverse Synthetic Aperture for emulated antenna array
See Through Wall: WiVi

● Property used
  ○ MIMO interference nulling at wall, first obstacle
  ○ Inverse Synthetic Aperture for emulated antenna array

● Objective achieved
  ○ Overcome flash effect
  ○ Have a portable solution
Tracking Keystrokes using Wireless Signals
Tracking Keystrokes using Wireless Signals
Tracking Keystrokes using Wireless Signals

![Graph showing 50 Key Stroke and Baseline Phase](image-url)
From phase to delay

- Get delay introduced by keystroke by converting phase shift into delay
- Capture delay effect by using cancellation at receiver
From delay to keystroke

- Measure trough location to infer change in channel
- Introduce artificial delay to make trough more significant
The keystroke tracking system

**Spectrum Analyzer**
1. Feedback control to adjust signal cancellation based on spectrum shape
2. Locate trough position as the index to key stroke detection

**Key stroke detection Algorithm**
Tracking Keystrokes: Performance

Repeated key 5 on keypad: accuracy
Tracking Keystrokes: Performance

Full key range, partially trained
Tracking Keystrokes using Wireless Signals

- Property used
  - Shift in frequency of cancellation through caused by phase shift of channel
  - Finger modeled as source of multipath signal
Tracking Keystrokes using Wireless Signals

- Property used
  - Shift in frequency of cancellation through caused by phase shift of channel
  - Finger modeled as source of multipath signal

- Objective achieved
  - first passive, single receiver keystrokes tracking system
  - agnostic of physical layer and MAC protocols
We Can Hear You with WiFi: WiHear

Device free, non-invasive remote ‘hearing’
We Can Hear You with WiFi

- Vowels and consonants
- Filtering
  - Remove Noise
  - Partial Multipath Removal
  - Profile Building
  - Wavelet Transform

Mouth Motion Profiling

- Laptop
- People
- MIMO Beamforming
- AP
Mouth motion profiling

- Locating mouth
Mouth motion profiling

- Filtering out-band interferences
  - cancel high frequency interferences
  - remove both static interferences and winking using band-pass filter (red boxes)
Mouth motion profiling

- Partial multipath removal
  - Convert Channel State Information to time domain via IFFT
Mouth motion profiling

- Partial multipath removal
  - Convert Channel State Information to time domain via IFFT
  - Remove multipath >500 ns
Mouth motion profiling

- Partial multipath removal
  - Convert Channel State Information to time domain via IFFT
  - Remove multipath >500 ns
  - Convert CSI back to frequency domain via FFT
Mouth motion profiling

- Partial multipath removal
  - Convert Channel State Information to time domain via IFFT
  - Remove multipath >500 ns
  - Convert CSI back to frequency domain via FFT

- Rational
  - mouth motion is non-rigid compared to other body movements
  - multipath reflections with similar delays do all contain information about the mouth motion
Mouth motion profiling

- Apply discrete wavelet packet decomposition
  - easier signal analysis on time and frequency domain
  - allows multi-scale analysis
Learning based lip reading
Learning based lip reading

- Word segmentation
- Inner-word segmentation
- Feature extraction
- Classification
We Can Hear You with WiFi

(a)  
(b)  
(c)  
(d)  
(e)  
(f)
We Can Hear You with WiFi

- Property used
  - MIMO beamforming, focused on mouth
  - Partial multipath effect, partially remove multipath after wavelet packet transformation
We Can Hear You with WiFi

- **Property used**
  - MIMO beamforming, focused on mouth
  - Partial multipath effect, partially remove multipath after wavelet packet transformation

- **Objective achieved**
  - Lip reading and speech recognition without line of sight
  - Context aware speech recognition enhancement
Conclusion

- All three very innovative
- Early stage proofs of concept
- Novel use cases requiring NLOS sensing
- Far reaching privacy implications
- The ISM band can be used for more than machine to machine communication, e.g. indoor localization, sensing and control
Follow up results

video src: https://youtu.be/sbFZPPC7REc?t=122
Follow up results

Our device can also monitor breathing and heart rate