

# Yuxuan Zhou

Email : yzhoudo@connect.ust.hk

Personal Website : <https://kevinous.github.io/>

Mobile : +86-15827447741; +852-59763172

Date of Birth: 1998.03 | Gender: Male



## EDUCATION

---

- **The Hong Kong University of Science and Technology** Hong Kong SAR, China  
*Ph.D. Candidate of Computer Science Engineering* *Sep. 2020 – 2025 (expected)*
  - **GPA:** 3.914/4.0
  - **Research Interest:** Wireless Sensing, Smart Health, Security and Privacy, Reconfigurable Intelligent Surface (RIS) aided Sensing, Internet of Thing
  - **Honors:** HKUST Postgraduate Scholarship, Research Travel Grant
- **Huazhong University of Science and Technology** Hubei, China  
*Bachelor of Electronic and Information Engineering* *Sep. 2016 – July. 2020*
  - **GPA:** 3.93/4.0 (Rank: 1/29, experimental class in Qiming College)
  - **Honors:** National Scholarship, Merit Student Scholarship, Outstanding Undergraduate, HNA Group Scholarship, Excellent Social Practice of University, Scholarship for Scientific and Technological Innovation, Successful Participant of MCM

## RESEARCH PROJECTS

---

- **Parkinson's Disease Tremor Monitoring with mmWave Radar** *Oct. 2023-present*  
*Ongoing, Leader*
  - **Motivation:** Contactless Parkinson's Disease (PD) tremor in-home monitoring is important for reducing hospital visits, enabling personalized treatment plans, and providing a more accurate representation of a patient's tremors in their natural environment, ultimately leading to better treatment outcomes. This project aims to develop a non-invasive solution to monitor the tremor of PD patients.
  - **Methodology:** We incorporate a depth camera to compensate for the low angle resolution of mmWave radar, and we also propose a novel learning-based method to assess the amplitude of the tremor accurately.
- **Physical Attack against WiFi-based Intrusion Detection via RIS** *Feb. 2022 - Dec. 2022*  
*ACM Sensys 2023, Leader*
  - **Motivation:** The emergence of Reconfigurable Intelligent Surface (RIS) technology has brought about significant improvements in wireless communication, but it may also introduce new security threats to wireless sensing systems. This project aims to develop a practical attack that can expose the vulnerabilities of these systems to RIS-aided attacks in real-world scenarios.
  - **Methodology:** We propose a practical and covert attack that renders moving individuals undetectable by WiFi-based intrusion detection systems in real-life scenarios. The attack combines motion reduction and threshold lifting strategies to overcome challenges such as limited RIS affordability, constrained cooperation in adversary settings, and complex and unpredictable environments.
- **RIS-aided Multi-user Indoor Localization Using COTS WiFi** *Mar. 2022 - Nov. 2022*  
*ACM Sensys 2023, Member*
  - **Motivation:** Multi-user indoor localization is a valuable wireless application that requires low latency and high robustness to dynamic interference from surrounding people. However, current state-of-the-art systems cannot simultaneously achieve both of these essential requirements, creating a need for a more efficient and reliable solution.
  - **Methodology:** We use RIS for WiFi beam scanning, allowing clients to determine their direction in a single scan. To handle the complex signal superposition at the receiver, we utilize the reconfigurability of RIS to give target beams distinguishing features, enabling RIScan to extract stable and accurate direction information from dynamic environments.

## • **Adversarial Attack against WiFi-based Gesture Recognition System**

*ACM IMMUT/Ubicomp'22, Leader*

*Nov. 2020 - Oct. 2021*

- **Motivation:** The security vulnerabilities of these systems, which stem from the open nature of the wireless medium and the inherent defects of Deep Learning, have not been sufficiently investigated. This project aims to develop an attack that reveals the vulnerability of these systems, highlighting the need for improved security measures.
- **Methodology:** We incorporate a signal synthesis scheme and a black-box attack scheme to generate adversarial signals with desired motion features and handle inconsistencies between the perturbation space and input space of the classifier, respectively.

## TALKS

---

- **WiAdv:** Practical and Robust Adversarial Attack against WiFi-based Gesture Recognition System, UbiComp 2022, Cambridge, UK, 2022.09
- **RIS stealth:** Practical and Covert Physical-Layer Attack against WiFi-based Intrusion Detection via Reconfigurable Intelligent Surface, SenSys 2023, Istanbul, Turkey, 2023.11

## SKILLS

---

- **Coding:** Matlab, Python, C, C++, Golang
- **Techniques:** Signal Processing, Data Analysis, Deep Learning

## PUBLICATIONS

---

- **Yuxuan Zhou**, Chenggao Li, Huangxun Chen, and Qian Zhang. 2023. RIS stealth: Practical and Covert Physical-Layer Attack against WiFi-based Intrusion Detection via Reconfigurable Intelligent Surface. ACM Conference on Embedded Networked Sensor Systems (SenSys) 2023.
- Chenggao Li, Qianyi Huang, **Yuxuan Zhou**, Yandao Huang, Qingyong Hu, Huangxun Chen, and Qian Zhang. 2023. RIScan: RIS-aided Multi-user Indoor Localization Using COTS WiFi. ACM Conference on Embedded Networked Sensor Systems (SenSys) 2023.
- **Yuxuan Zhou**, Huangxun Chen, Chenyu Huang, and Qian Zhang. 2022. WiAdv: Practical and Robust Adversarial Attack against WiFi-based Gesture Recognition System. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. 6, 2, Article 92 (July 2022), 25 pages.