IEEE Hong Kong 6G Wireless Summit

11-12 September 2024
Hong Kong, China

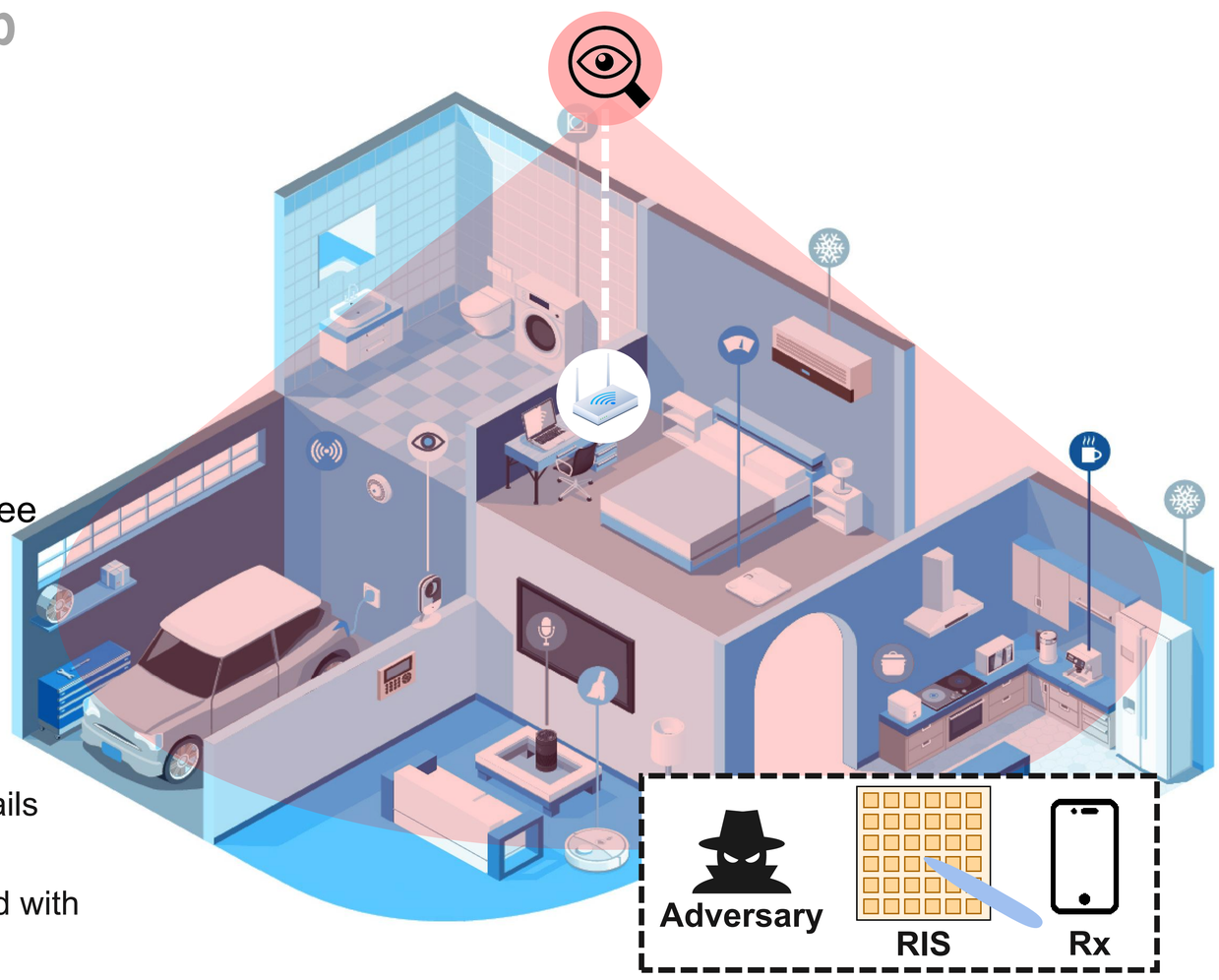
IEEE ComSoc IEEE Communications Society | IEEE

Department of Computer Science and Engineering, HKUST

RIStealth: Practical and Covert Physical-Layer Attack against WiFi-based Intrusion Detection via Reconfigurable Intelligent Surface

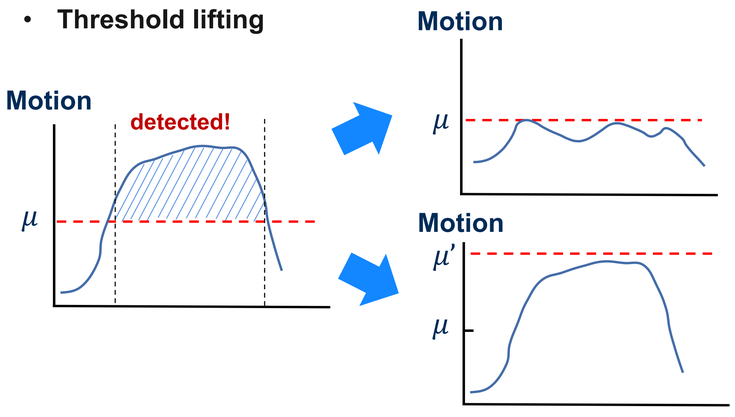
Yuxuan Zhou, from Prof. Qian Zhang's Group

- WiFi signals are suitable for home intrusion detection
  - Privacy-preserving and unobtrusive
  - Severe consequences may arise if compromised or malfunctions
- Reconfigurable Intelligent Surface (RIS)
  - Represents a paradigm shift from passive channel measurement to proactive channel customization
  - Potentially enables stronger attack methods
- We propose a practical and robust physical-layer attack with three challenges:
  - **Limited Affordability of Practical RIS**
    - Limited size of the RIS for stealth and mobility
    - Restricted signal manipulation space due to the size
  - **Restrained Cooperation in Adversary Setting**
    - The benign transceivers will not help the RIS with deployment details
  - **Complex and Unpredictable Environment**
    - The area being intruded upon may be a complex environment filled with unknown reflectors, such as furniture and metal objects

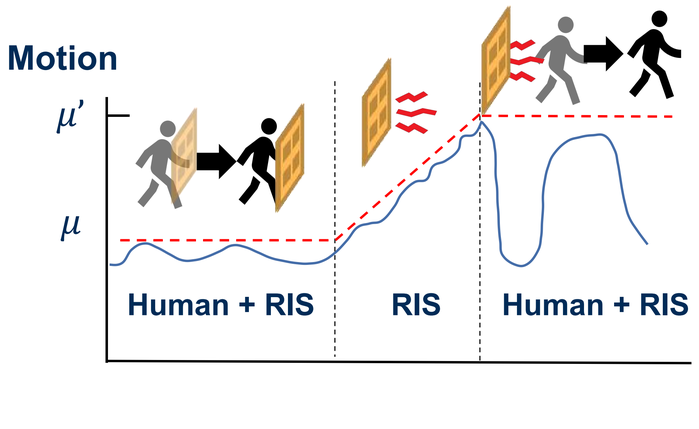


Observation

- Two methods to avoid detection by intrusion detection systems
  - **Motion reflection reduction**
  - **Threshold lifting**

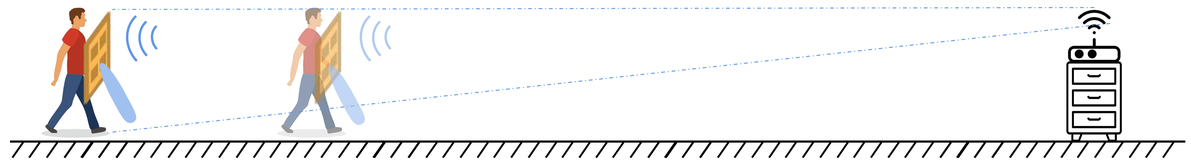


- **RIStealth** combine **motion reflection reduction** and **threshold lifting** to form a practical attack scheme
  - Motion reflection reduction is more suitable for distant areas
    - Prevent triggering alarms due to uncovered limbs
  - Threshold lifting is more effective for nearby areas
    - Maximize the limited signal manipulation capability

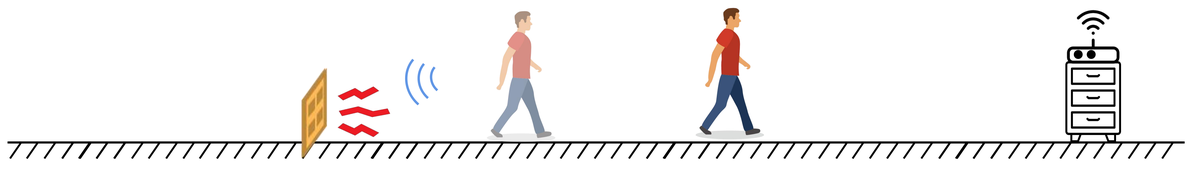


RIStealth Workflow

- **RIStealth** consists of two phases: **Sneaking Phase** and **Radio Blast Phase**



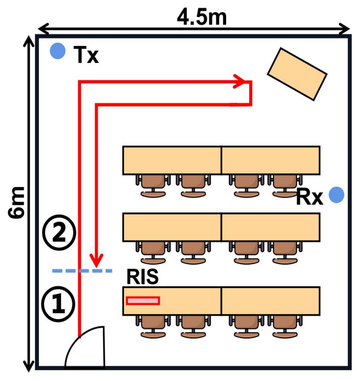
- **Sneaking Phase:** keep covert until reaching the switching point to the **Radio Blast Phase**
  - Leverages pre-measured rough system information to redirect the WiFi signal toward the ground
  - Avoids unpredictable multipaths using our proposed beam broadening method

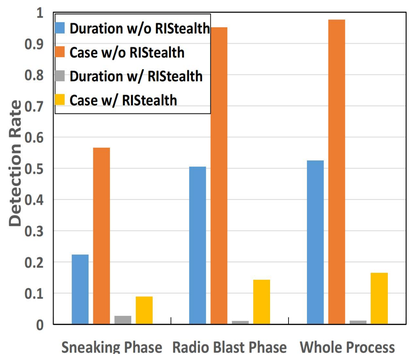


- **Radio Blast Phase:** lift the threshold so that subsequent movements of the attacker will not be detected
  - Accurately localizes the benign transmitter with our novel RIS component extraction method
  - Creates artificial noise using our proposed configuration strategy to gradually increase the detection threshold

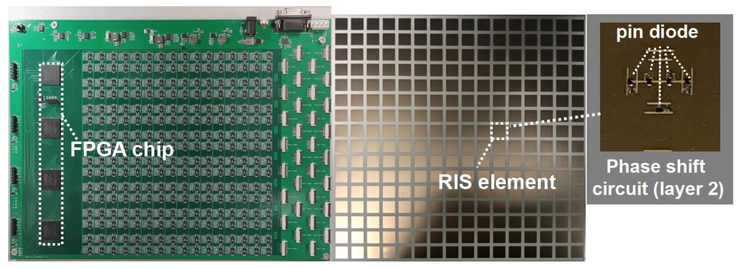
Evaluation Results

- End-to-end line-of-sight (LOS) evaluation
  - Launch **Sneaking Phase** in ① and **Radio Blast Phase** in ②
  - Assess with case detection rate and duration detection rate





- Implement with a 16×16 2-bit phase shifitng RIS prototype



- **RIStealth** decreasing the case detection rate of the victim system from **97.1%** to approximately **15%**
  - Validates the threat of RIS to wireless sensing
  - Promotes advancements in RIS utilization and RIS-relevant security issues

Related Publications

Yuxuan Zhou, Chenggao Li, Huangxun Chen, and Qian Zhang. 2024. RIStealth: Practical and Covert Physical-Layer Attack against WiFi-based Intrusion Detection via Reconfigurable Intelligent Surface. In Proceedings of ***the 21st ACM Conference on Embedded Networked Sensor Systems (SenSys '23)***. Association for Computing Machinery, New York, NY, USA, 195–208, https://doi.org/10.1145/3625687.3625790

Acknowledgment

This work was supported in part by the Hong Kong Research Grants Council under the Areas of Excellence Scheme Grant AoE/E-601/22-R