

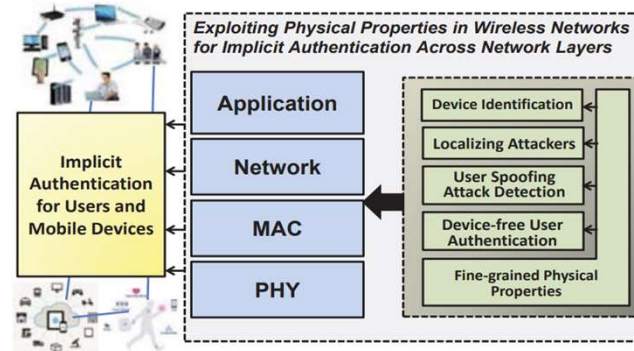
Exploiting Physical Properties in Wireless Networks for

Implicit Authentication



Challenge:

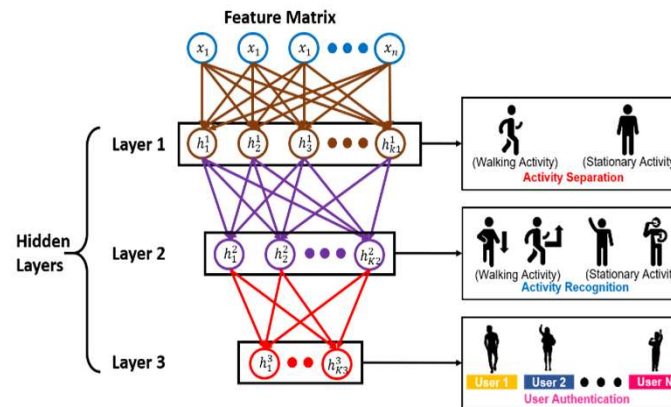
- Existing user/device authentication either employing specialized or expensive hardware or requiring users' active involvement
- Achieve low-cost and unobtrusive authentication without the users' active participation



Framework of implicit authentication in wireless networks`

Solution:

- Leverage fine-grained wireless signatures (i.e., CSI) and the corresponding spatial correlation of mobile devices as unique physical properties to enhance implicit authentication
- Device-free User Authentication:** Identify unique physiological and behavioral characteristics from human leveraging fine-grained wireless signal properties
- User Spoofing Detection and Attacker Localization:** Achieve trustworthy communication among connected devices through effective user authentication and localizing user-spoofing attackers
- Accurate Device Identification:** Secure communication among connected devices by capturing the characteristic of device-specific radio signatures



Deep learning-based model for user authentication

Scientific Impact:

- Advance knowledge in exploiting physical layer information for securing corporate and home environments
- Contribute to the successful development and adoptions of customized applications involving wireless devices
- Implement and validate the proposed strategies by prototyping the framework with commodity hardware

Broader Impact:

- Advance the foundation of exploiting Wi-Fi signals to assist security solutions
- Include curriculum development, outreaching to K-12 students
- Facilitate a variety of emerging wireless applications

#1717356: SaTC: CORE: Small: Collaborative: Exploiting Physical Properties in Wireless Networks for Implicit Authentication
 PIs: Yingying Chen (Rutgers University), Hongbo Liu (Indiana University Purdue University Indianapolis),