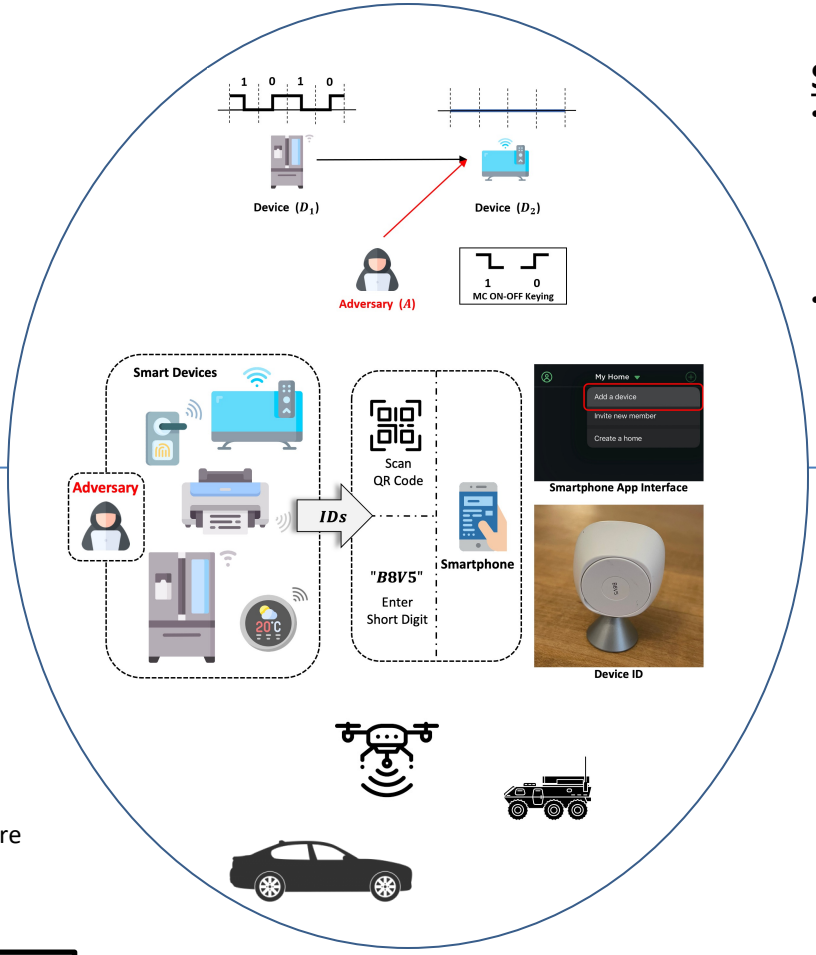
Toward Usable and Ubiquitous Trust Initialization and Secure Networking in Wireless Ad Hoc Networks

Challenge:

- To bootstrap trust among devices with limited or zero trust, major challenges exist in multiple folds including
  - light-weight design
  - high usability
  - minimal hardware modification for compatibility with commodity devices
  - strong attacks such as man-in-the middle attacks and wireless signal modification.

Solution:

- *Authentication by presence* to thwart strong attacks including wireless signal modifications; PHY-layer secret key generation that maximize secrecy capacity utilizing environmental randomness.
- Main innovations include novel device authentication techniques based on in-band transmission randomization, and new secret-key generation methods based on mobility-induced context-aware channel characteristics



Scientific Impact:

- This research addresses an important problem of trust initialization in hostile environments where limited or zero-trust exists. The proposed solutions advance the research in lightweight wireless security especially PHY-layer security.
- The project involved security design and vulnerability study of commodity wireless devices, which extends the community's understanding of attackers' capability and the potential of PHY-layer security

Broader Impact and Broader Participation:

- This project has generated a suit of lightweight and usable security protocols for in-band device authentication and secret-key generation. This research has resulted in 3 published papers and 2 in preparation.
- The research is aimed for usable security protocols compatible with commodity devices. Therefore, it has the potential to transition to practice.
- The project has provided research opportunities for 6 graduate students including 1 graduated PhD student. Among the 6 students 3 are female.

NSF SaTC #1817438;

PI: Shucheng Yu (shucheng.yu@stevens.edu)
Institution: Stevens Institute of Technology