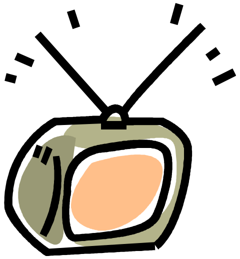
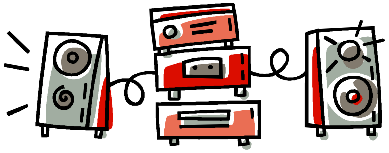
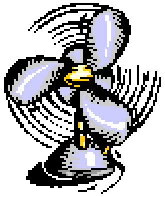
NSF NextG Security Workshop

The “Physical” Layer







Lee Swindlehurst
University of California Irvine

NSF NextG Security Workshop

- **Physical Layer Security**
  - ➢ Ugly step-child of the security world
  - ➢ But has a compelling story:

    not subject to computational advances
    natural shared randomness in wireless channel
    perfect secrecy is theoretically possible

- **Many advances of this decade have found their way to practice**
  - ➢ Massive MIMO
  - ➢ NOMA
  - ➢ Hybrid beamforming
  - ➢ Cell-free or distributed MIMO, etc.

- **Why not PLS?**
  - ➢ CSI often assumed for adversary (req'd for secrecy metrics)
  - ➢ Strong assumptions about adversary => insistence on perfect secrecy
  - ➢ Design for worst case, conservative solutions
  - ➢ Emphasis on secrecy performance, not on desired link reliability
  - ➢ Artificial noise/jamming not appropriate in interference-limited scenarios
  - ➢ capability of PHY-generated keys is often limited
  - ➢ cryptographic methods aren't chopped liver after all ….

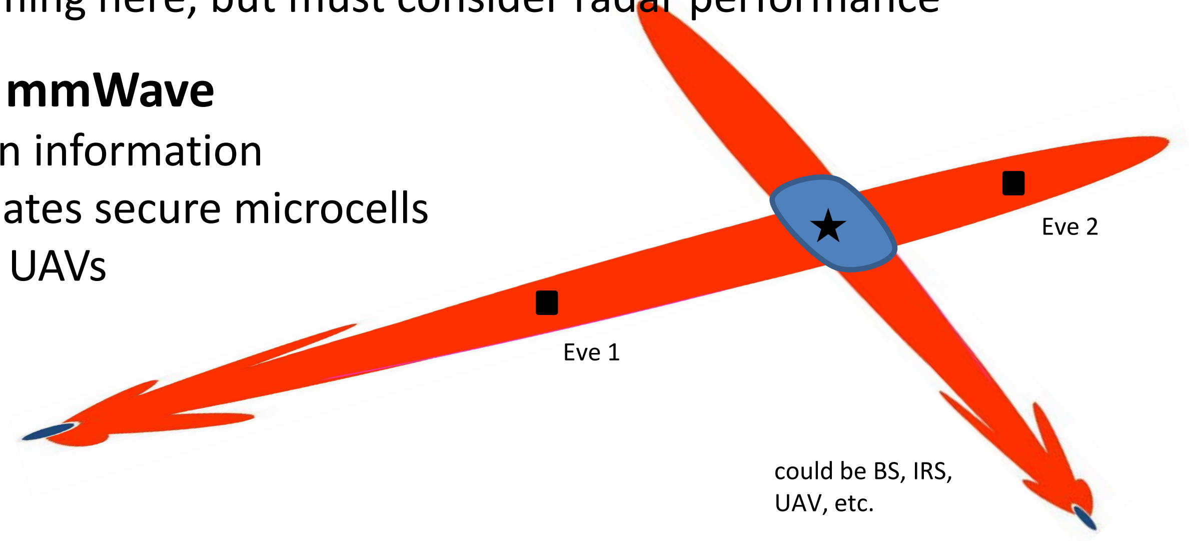
Some Reasons for Optimism

- **5G and IoT**
  - ➢ may require lightweight security, room for PLS
  - ➢ emphasis on reliability, delay, massive connectivity

    guaranteed low-rates, fixed constellations => finite alphabet metrics
    PLS is a plus for latency
    connectivity => exploit multi-user interference to hide sensitive data
    constructive interference, symbol-level precoding

- **Vehicular Networks**
  - ➢ We know where the adversaries are
  - ➢ ….. and we communicate with them!
  - ➢ A role for AN/jamming here, but must consider radar performance

- **Distributed MIMO & mmWave**
  - ➢ CSI reveals location information
  - ➢ Wide aperture creates secure microcells
  - ➢ Also possible with UAVs



could be BS, IRS,
UAV, etc.

Some Reasons for Optimism

- **Heuristic approaches**
  - fountain codes, exploits asymmetric decoding success
  - combine RF and biometric fingerprinting for authentication, key generation
  - AI/ML as a tool to extract common information for PHY keys
  - non-linear precoding