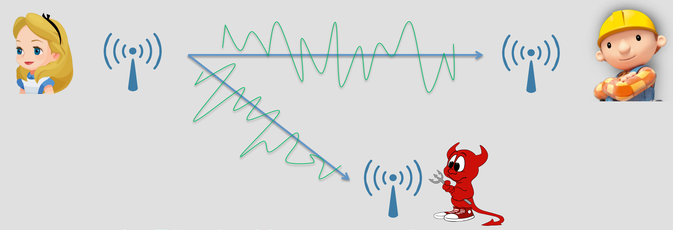
Wireless Physical Layer Security

P. Mukherjee and S. Ulukus

30 THIRTY YEARS OF SYSTEMS RESEARCH EXCELLENCE

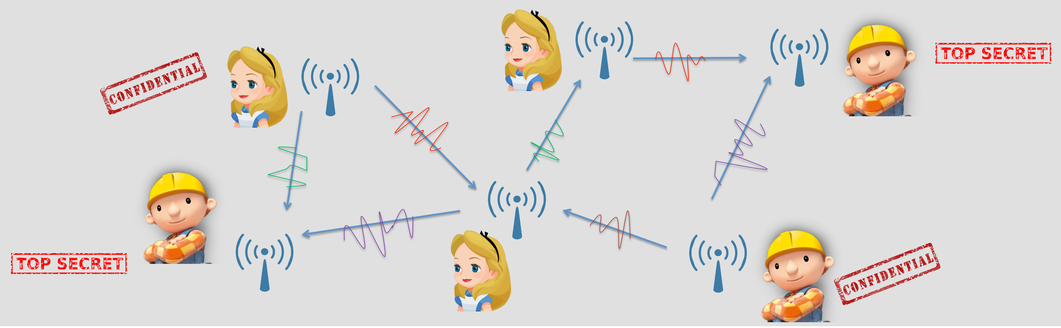
INSTITUTE FOR SYSTEMS RESEARCH
A. JAMES CLARK SCHOOL OF ENGINEERING

- Traditional approach to security: Cryptography
  - Based on the assumption of limited computational power at eavesdropper
  - May be inadequate against large scale quantum computers

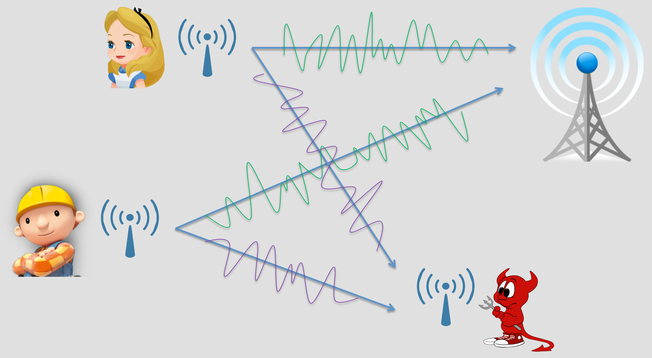


- Alternate approach: Physical layer security
  - Provable and quantifiable using an information theoretic framework
  - Exploits channel characteristics inherent to wireless medium (e.g., fading)

- Multi-user cooperation in general network topologies.
- Cooperative jamming with delayed and imprecise CSI.
- Explicit code design for physical layer security in wireless networks.

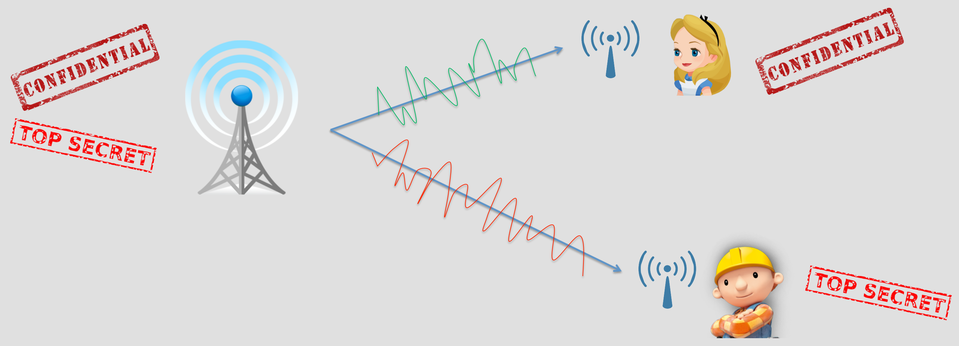


- Key objective: Create channel advantage by:
  - Time, frequency, multi-antenna and multi-user diversity
  - Multi-user cooperation and signal alignment
- Crucial ingredient: Channel state information (CSI) at the terminals



- Channel gains are measured at receivers and fed back to transmitters periodically
- Eavesdropper may or may not provide its channel gains to transmitters.
- For the K-user multiple access wiretap channel, maximum sum secure throughput:
  - With eavesdropper's CSI: $\approx \frac{K(K-1)}{K(K-1)+1}\log\text{SNR}$
  - Without eavesdropper's CSI: $\approx \frac{K-1}{K}\log\text{SNR}$
- **Conclusions**:
  - Even without eavesdropper's CSI and using only single antenna terminals, positive secure rate that scales with SNR.
  - The cost of security decreases as number of users increases.
  - User-cooperation is beneficial to every user.

- CSI fed to the transmitters is imprecise and delayed in practice.
- Focus on the delay aspect:
  - Model it as either instantaneous or completely stale or unavailable
  - CSI, when available is precise



- The base station has 2 antennas, receivers have single antennas.
- The maximum sum secure throughput:

	instantaneous	completely stale	unavailable
instantaneous	$2\log\text{SNR}$	$\log\text{SNR}$	$\log\text{SNR}$
completely stale	$\log\text{SNR}$	$\log\text{SNR}$	$\frac{1}{2}\log\text{SNR}$
unavailable	$\log\text{SNR}$	$\frac{1}{2}\log\text{SNR}$	$o(\log\text{SNR})$

- **Conclusions:**
  - Even completely stale CSI can be very useful.
  - Tells us the minimum CSI requirement for a given rate.
  - Multiple antennas at the transmitter is very useful.

Funding sources: NSF, ARL

Joint work with J. Xie, E. Ekrem, R. Bassily, R. Tandon, S. Shafiee and N. Liu

CSPL Communication and Signal Processing Laboratory