The Fading Multiple-Access Wire-Tap Channel

Ender Tekin and Aylin Yener

❖We live in a wireless world (e.g. Wi-Fi, cell phones, RF-ID chips), which means that our communications channel is:

➢Easy to tap without being detected; and

➢Unprotected against jamming.

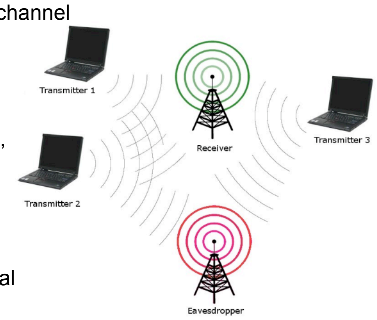
❖Thus far, the design of wireless networks has been guided solely by efforts to increase capacity, however, there is a dire need to incorporate ***security*** in design.

➢For example, the security of e-banking and e-shopping applications is of far greater importance than the data transmission rates of these transactions.

❖The security issue is traditionally left to the upper layers, but we need to incorporate security into the actual *physical layer* design of wireless communications systems to address the following problems:

➢Design of *provably secure* systems;

➢Encryption may be unfeasible for small, simple nodes.



Design Goal: Maximizing sum-rates while keeping communications **secure** in the presence of an intelligent and informed eavesdropper.

Cooperative Secrecy

❖Achievable secrecy sum-rate using “wire-tap codes” is the difference of the sum-capacities of the main and eavesdropper channels:

$$R_{sum}^{s} = C_{sum}^{\text{main}} - C_{sum}^{\text{eavesdropper}}$$

❖Since both terms are a function of transmit powers, we can optimize the secrecy sum-rate over the transmit powers.

➢Users with better eavesdropper channels cease transmission,

➢Users with better main channel gains transmit with maximum power.

❖Can these idle users somehow help?

➢Observe: These idle users can jam the eavesdropper very effectively.

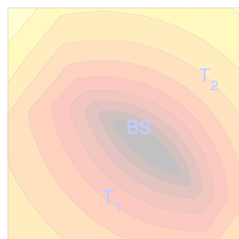
➢Even though jamming hurts the intended receiver as well, since it hurts the eavesdropper more, the secrecy sum-rate increases!

❖**Cooperative Jamming**: Optimum power allocation is such that the

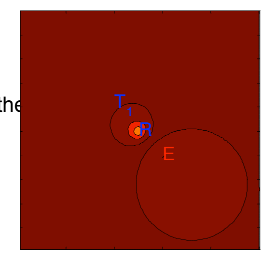
➢strongest users transmit with maximum power,

➢the weakest users jam with maximum power,

➢one limiting user jams with nonzero/nonmaximum power.



Secrecy sum-rates vs. eavesdropper location in geographic area for 2 use



Sum-rates vs. T_2 location in geographic area for 2 users w/ and w/o secre

Fading Wire-Tap Channels

❖Practical wireless scenarios incur fading.

❖We consider slow, ergodic block-fading.

❖In fading channels, it is optimal for a user to

➢save their power during deep fades,

➢transmit only when the channel gain is greater than a threshold. $h \geq \lambda$

➢Water-filling power allocation.

❖In multiple-access channels, it is capacity-optimal for only the **best** user to transmit at any given fading block.

❖2-user *fading wire-tap* channel:

➢Generally, a user only transmits if the *difference* of the main and eavesdropper channel gains exceeds a threshold, i.e., $h_k^{\text{main}} - h_k^{\text{eavesdropper}} \geq \lambda$

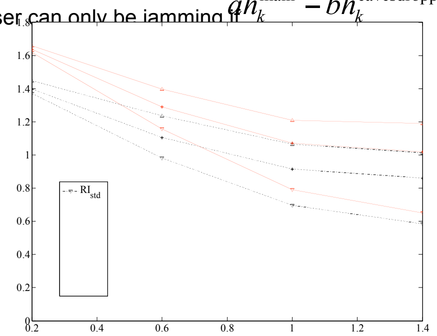
➢Sometimes it is optimal for both users to be transmitting!

❖**Cooperative Jamming**: decreases the necessary *effective* thresho

➢A user can only be transmitting if for some $a > b > 0$

$$a h_k^{\text{main}} - b h_k^{\text{eavesdropper}} \geq \lambda$$

➢A user can only be jamming if $a h_k^{\text{main}} - b h_k^{\text{eavesdropper}} < 0$



This research is being sponsored by NSF and DARPA ITMANET Program