Securing a wireless connected future

THE OHIO STATE UNIVERSITY

Aylin Yener

Roy and Lois Chope Chair
Electrical and Computer Engineering
Integrated Systems Engineering
Computer Science and Engineering

yener@ece.osu.edu

https://u.osu.edu/inspire/

THE OHIO STATE UNIVERSITY
COLLEGE OF ENGINEERING

INSPIRE@OHIOSTATE

Information & Networked Systems Powered by Innovation & Research in Engineering

Home INSPIRE Website

Home

INSPIRE@OhioState is a research group that consists of Prof. Yener and her research students.

The mission of INSPIRE is to conduct research in **foundations of Networked Systems**. Networked systems is a broad term that refers to **connected entities that communicate, compute, interact and learn**. Our vision calls for a connected world where **information flow is secure, reliable and sustainable.**

Core research disciplines and tools that we engage include information theory, optimization, machine learning, communication theory and signal processing.

Our focus is on system level design insights drawn from characterization of fundamental performance limits of such systems. We are also interested in developing algorithms approaching or achieving optimal design criteria.

There are diverse applications of our research in next generation AI, multi-genre networks, content delivery networks, as well as wired and wireless communication networks, Internet of Things (IoT) and energy-sustainable networking. Current more specifics topic areas are:

INSPIRE @OHIOSTATE

NEWS

Please refer to INSPIRE Website for more

Search this blog…

INSPIRE Current Research Foci

- 6G wireless
- AI for wireless
- Information security and privacy
- Content delivery networks
- Distributed and federated learning
- Distributed and edge computing
- Age of Information
- Energy-sustainable communication networks
- Vehicular network security

2G, 3G, 4G, 5G, ???

Each generation has a defining application innovation.

2G. digital communication; 3G. introduction of data
4G. unification and “high”-rate data services

5G. flexibility (network slicing); new spectrum

LTE on steroids or a game changer?

~10 year evolution?

Perhaps time to (seriously) think 6G?

What could 6G be about

Disruptive ~~technologies~~ ➔Disruptive design techniques

- Security provided by wireless signals
- …

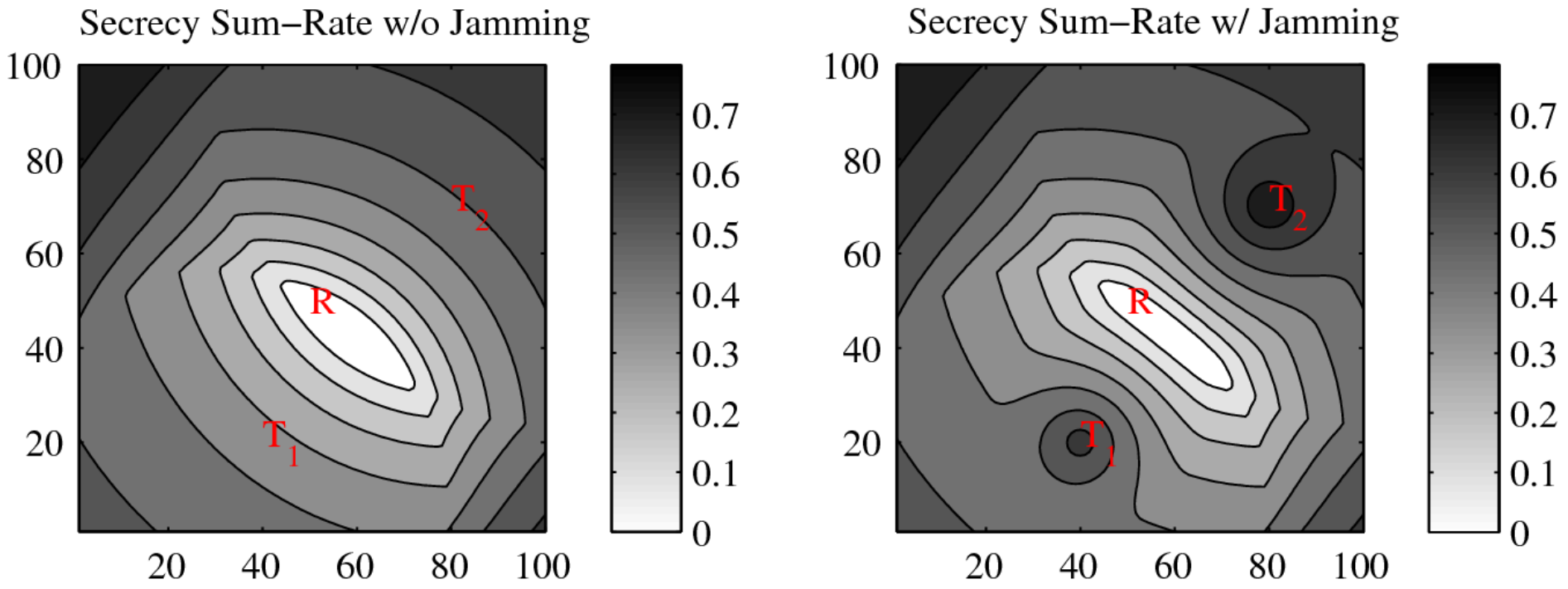
Rationale:

- Wireless has unique features, why not exploit them for security?
- We "optimize" wireless PHY for reliability, why not for security too?

Wireless Physical Layer Security

- **Broadcast medium (thus its vulnerabilities) unavoidable.**
- **PHY security exploits the medium to turn vulnerabilities into advantages.**
- **Example: Design judicious interference to thwart eavesdropping attacks (against computationally unbounded adversaries).**

Cooperative Jamming [Tekin-Y. 2006]



When Eve is close to one transmitter, that transmitter can hurt Eve more leading to a higher secrecy sum rate than if it tried to communicate.

PHY Security Realities

- PHY security is **information theory based as is PHY reliability.**
- **PHY security is secure against an adversary that KNOWS the everything about the system.**
- **Real cost: Rate penalty**
- **PHY security can be essential for scenarios of whenever massive and ultra fast key exchanges are impractical.**
  - **large dynamic networks with lightweight devices.**
  - **V2V/autonomous systems**
- **PHY security does not have to replace computational security, it can step in when needed (e.g. with software defined tx/nws)**

PHY Security Myths

- ~~PHY security cannot provide cryptographically sound guarantees.~~ PHY security is SEMANTICALLY secure.

- ~~PHY security does not work if adversary channels are not known.~~
  - Channel knowledge can be "compensated" by additional wireless resources [He-Y. 2014]
  - Channels can be "learned" without rate cost with the help of wireless sensing [Tahmasbi-Bloch-Y. 2019]

Bottomline: Computational security needs computational advantage, PHY security needs network advantage and wireless is the key to creating that advantage.

Example: Multiantenna PHY security [He-Y. 2014], [Nafea-Y. 2017]

- **Judicious interference can be good for security!**
  - **Structured interference** is good for securing wireless networks.
  - Align favorably at intended receiver AND unfavorably at the adversary.
- A road map for both confidential and anti-jam communications.
- Useful for applications that allow “alignment”.

V2X & Autonomous Systems