University of Delaware
November 16, 2011

Information & Inference in the Wireless Physical Layer

Vince Poor
(poor@princeton.edu)

Wireless Networks: Layers

Application (APP)	Web Browsing, Voice, etc.
Network (NET)	Routing, Flow Control, etc.
Medium Access Control (MAC)	Scheduling, Access Control, etc.
Physical (PHY)	Data Transmission

Research Trends in Wireless Nets

- The Past 25 Years: Key Developments at the PHY
  - *CDMA*
  - *OFDM*
  - *UWB*
  - *MUD*
  - *MIMO*
  - *Turbo*

Research Trends in Wireless Nets

- The Past 25 Years: Key Developments at the PHY
  - *CDMA*
  - *OFDM*
  - *UWB*
  - *MUD*
  - *MIMO*
  - *Turbo*
- Today: Focus on Interactions Among Nodes & Across Layers
  - *Among Nodes:*
    - Competition
    - Collaboration
    - Cooperation
  - *Across Layers:*
    - MAC-PHY
    - NET-PHY
    - APP-PHY

Research Trends in Wireless Nets

- The Past 25 Years: Key Developments at the PHY
  - *CDMA*
  - *OFDM*
  - *UWB*
  - *MUD*
  - *MIMO*
  - *Turbo*
- Today: Focus on Interactions Among Nodes & Across Layers
  - *Among Nodes:*
    - Competition
    - Collaboration
    - Cooperation
  - *Across Layers:*
    - MAC-PHY
    - NET-PHY
    - APP-PHY ← Information Transmission & Statistical Inference

Information & Inference in the Wireless PHY

Today's Talk: Four Problems in the Wireless PHY Motivated by the APP

- *PHY Security in Wireless Communication Networks*

  Motivated by Secure Information Transmission

- *Distributed Learning*

  Motivated by Statistical Inference in Wireless Sensor Networks

- *Finite-Blocklength Capacity*

  Motivated by Multimedia Information Transmission

- *Message Delivery in Small-World Networks*

  Motivated by Social Networking (Information & Inference)

Physical Layer Security in Communication Networks

Secure Information Transmission

[Joint work with Yingbin Liang, Shlomo Shamai, et al.]

Information & Inference in the Wireless PHY

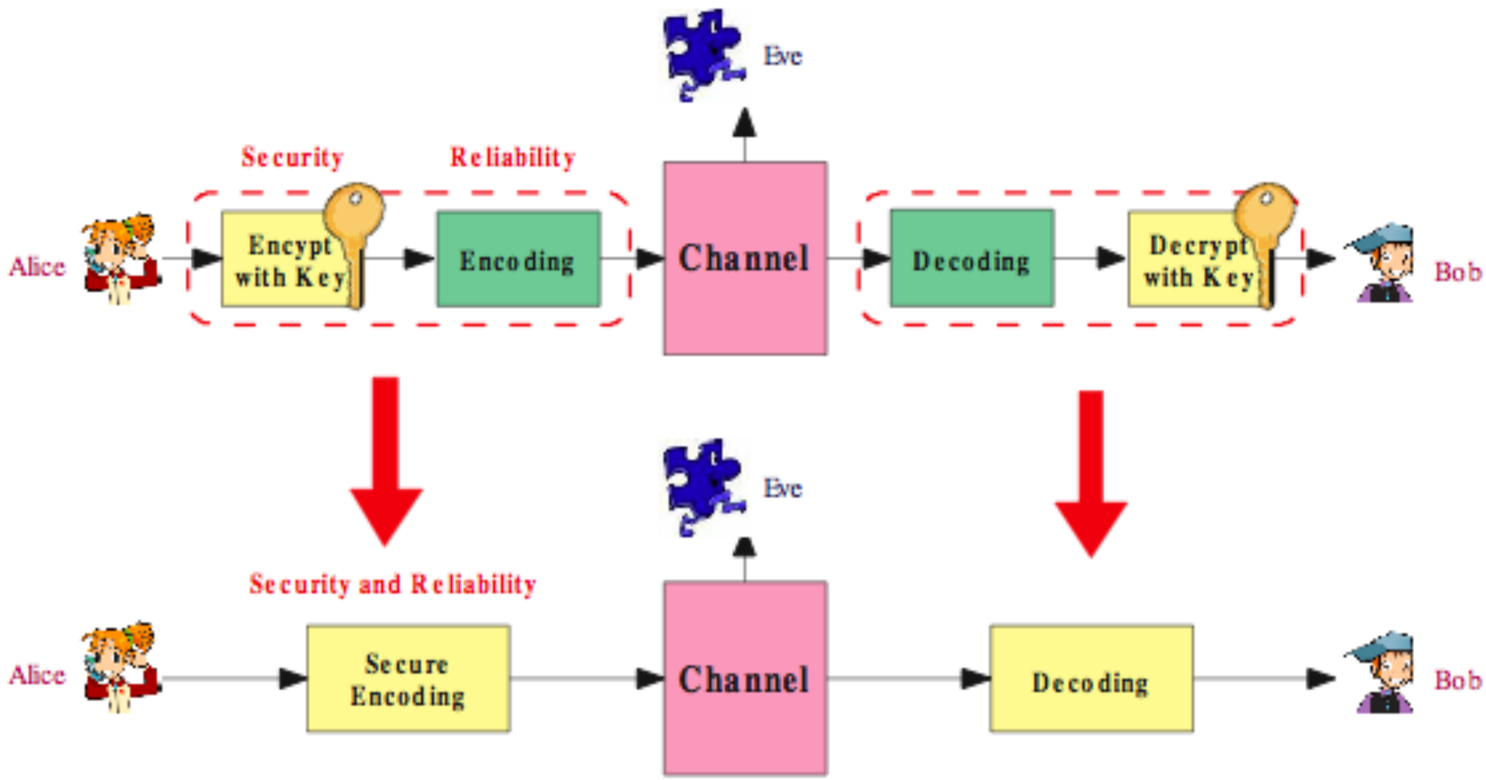
Motivation: Exploiting the PHY

- Key Techniques for Improving Capacity & Reliability:
  - *MIMO*
  - *Cooperation & Relaying*
  - *Cognitive Radio*

Motivation: Exploiting the PHY

- Key Techniques for Improving Capacity & Reliability:
  - *MIMO*
  - *Cooperation & Relaying*
  - *Cognitive Radio*
- What About Security?
  - *Traditionally a higher-layer issue (APP or Presentation)*
  - *Encryption can be complex and difficult without infrastructure*
  - *Information theoretic security examines the fundamental ability of the PHY to provide security*
  - *Caveat: This is still largely a theoretical issue*

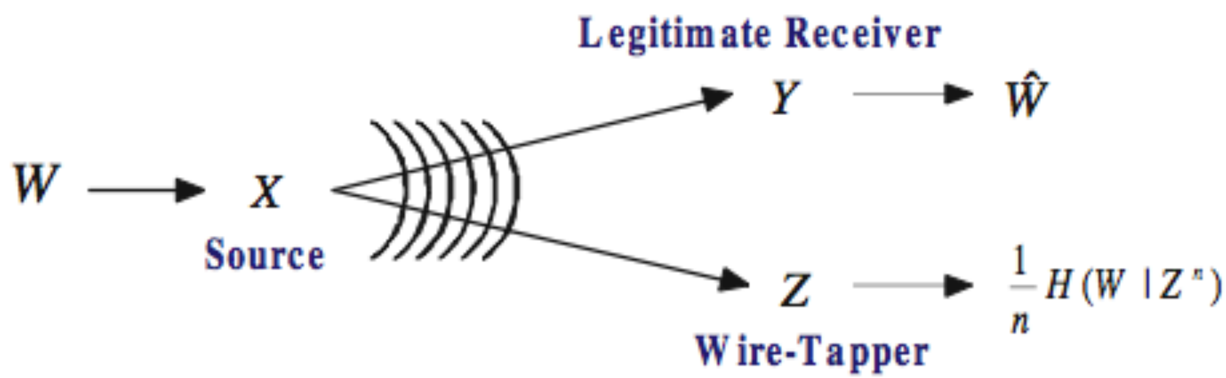
Physical Layer Security
Joint Encoding for Security and Reliability



A (Very) Brief History

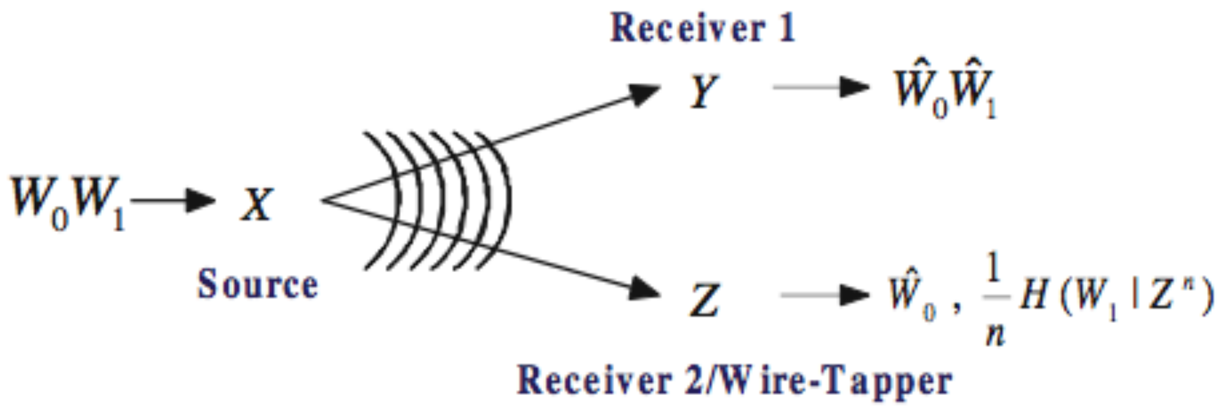
- Shannon [BSTJ'49]: For cipher, need *H(K) > H(S).*

- Wyner [BSTJ'75]: For the wire-tap channel



the wire-tapper must be degraded.

Broadcast Channel with Confidential (BCC) Messages

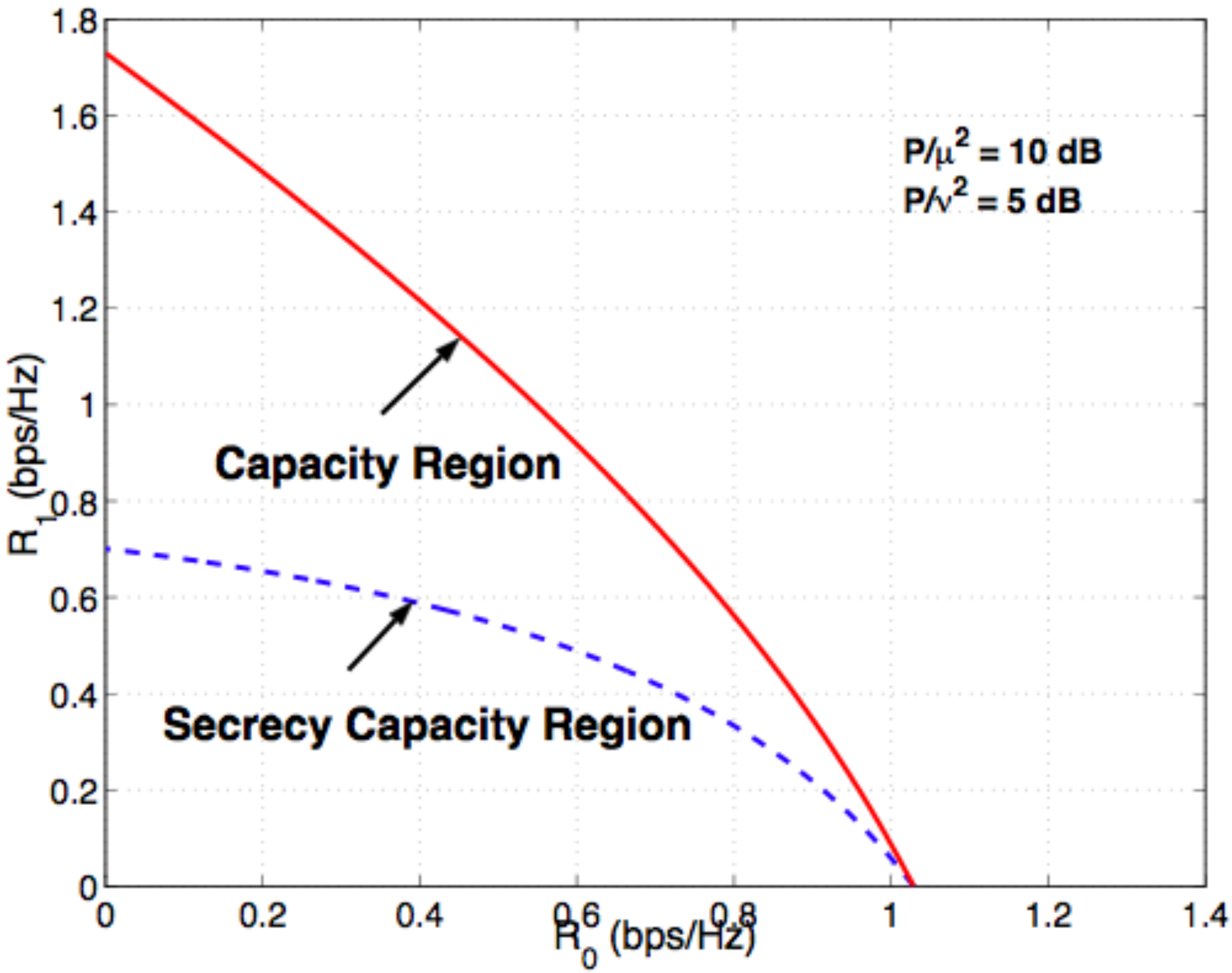


Csiszár & Körner [IT'78]: Discrete Memoryless BCC

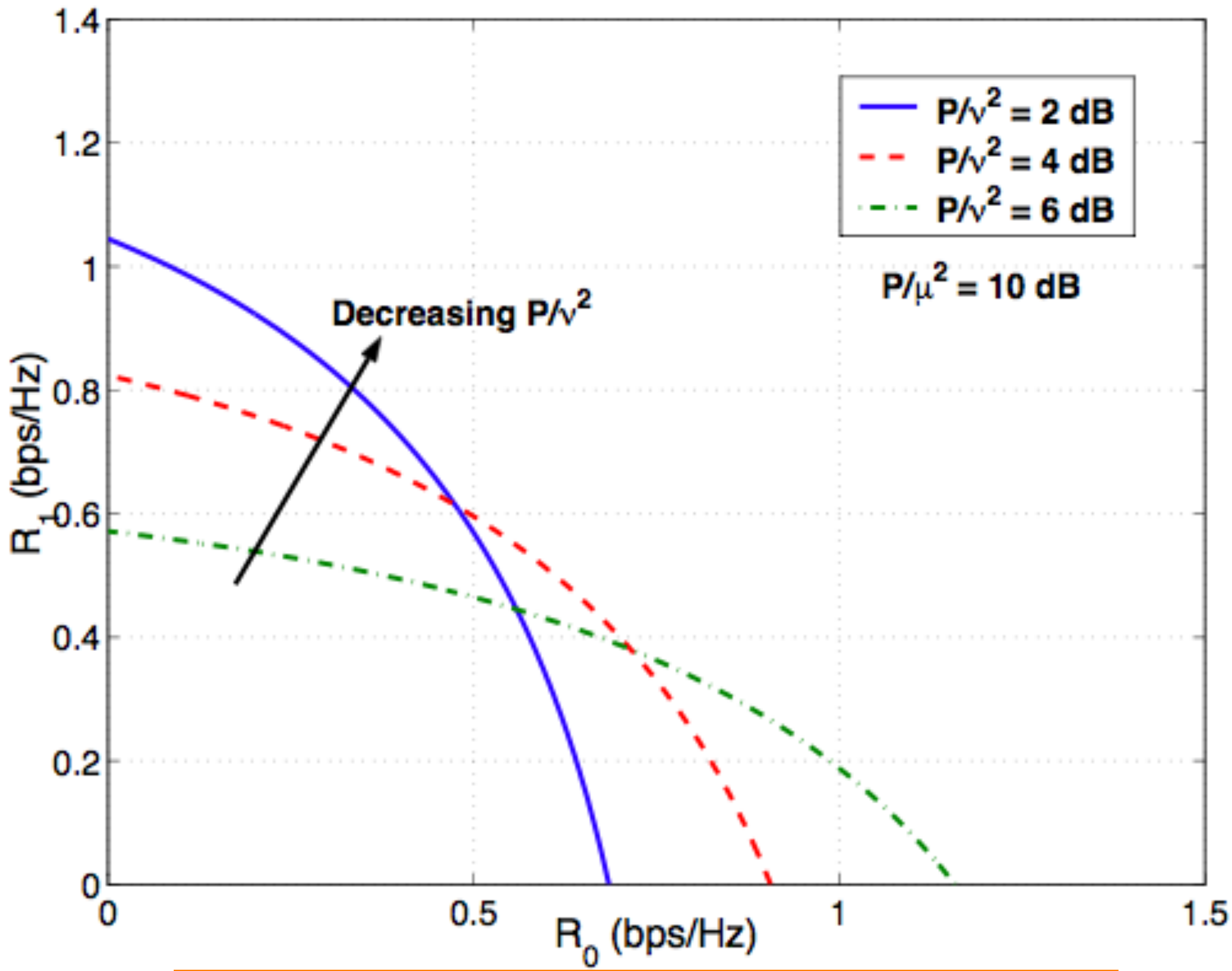
Liang, Poor & Shamai [IT'08]:

- Gaussian BCC
  - secrecy-capacity region
- Fading BCC
  - secrecy-capacity region
  - exploit fading to achieve secrecy
  - cptimal power allocation

Gaussian BCC

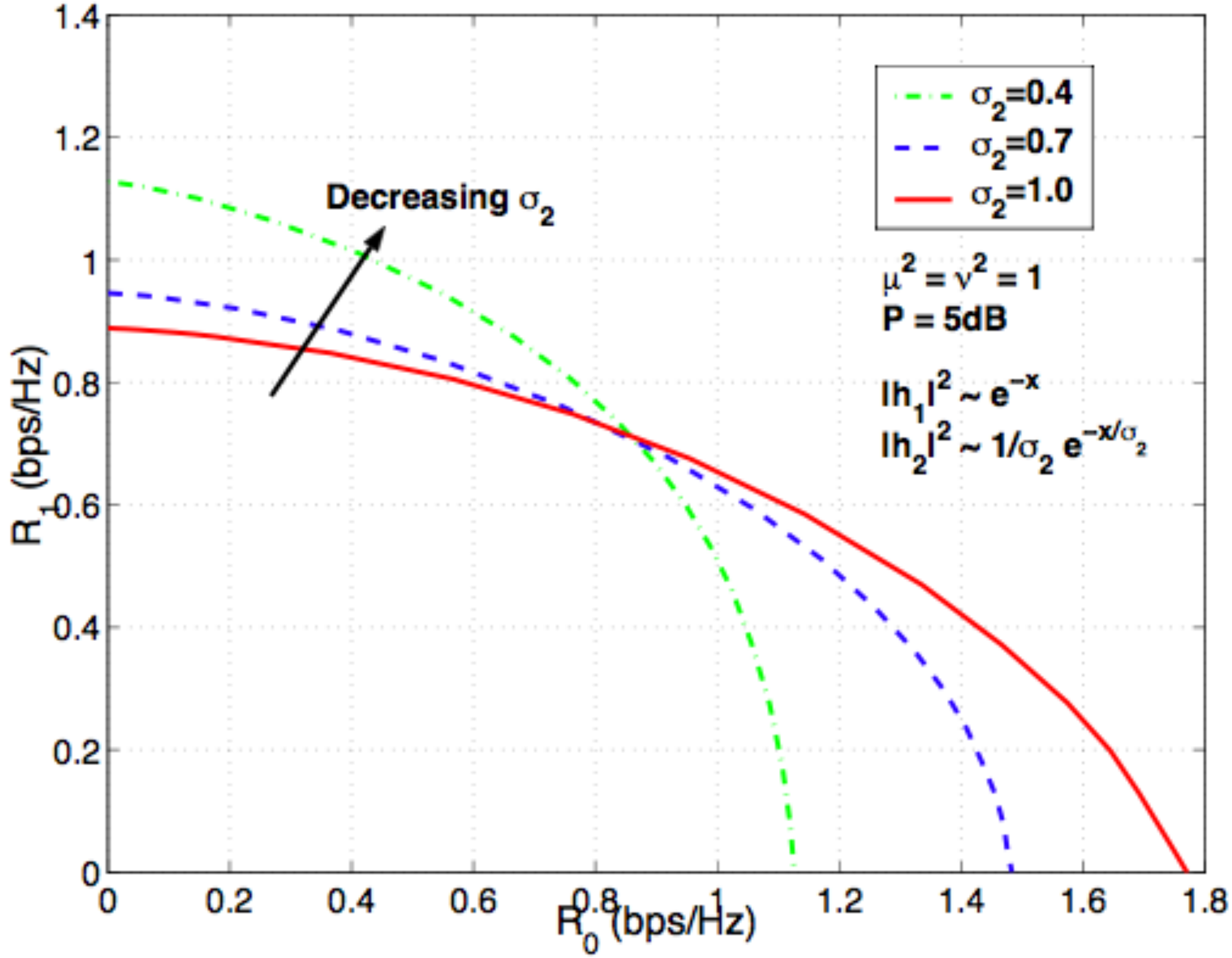


Gaussian BCC: Secrecy Capacity Regions

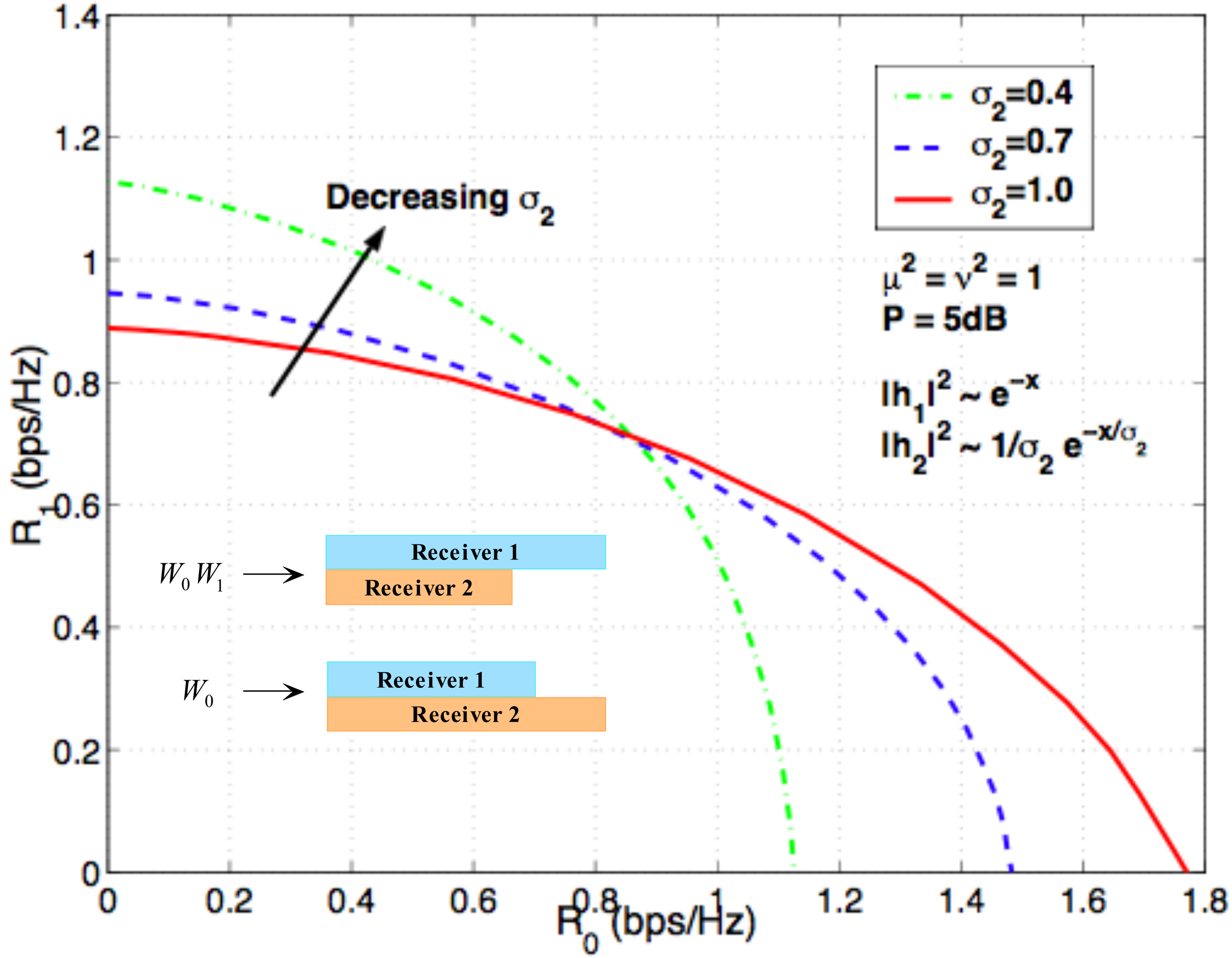


PHY Security in Wireless Communication Nets

Fading BCC: Secrecy Capacity Regions



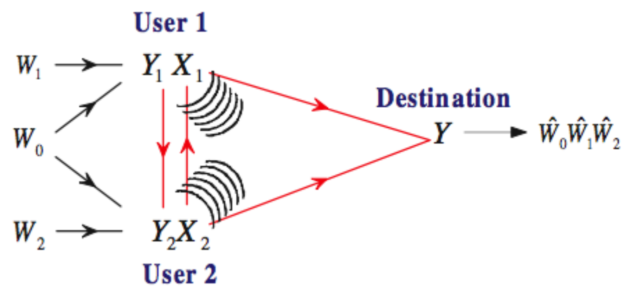
Fading BCC: Secrecy Capacity Regions



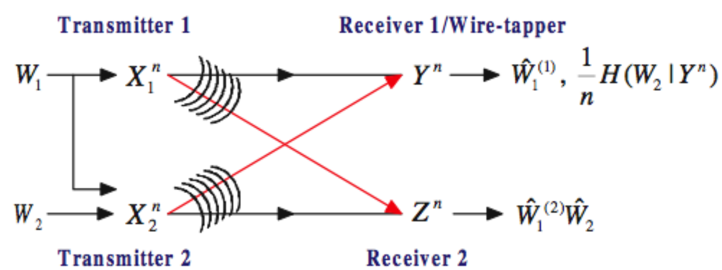
PHY Security in Wireless Communication Nets

Other Channels of Interest

- <u>Multiple-Access Channel</u> [w/ Liang - IT'08 (Gaussian); w/ Liu, Liang – IT'11 (fading)]:



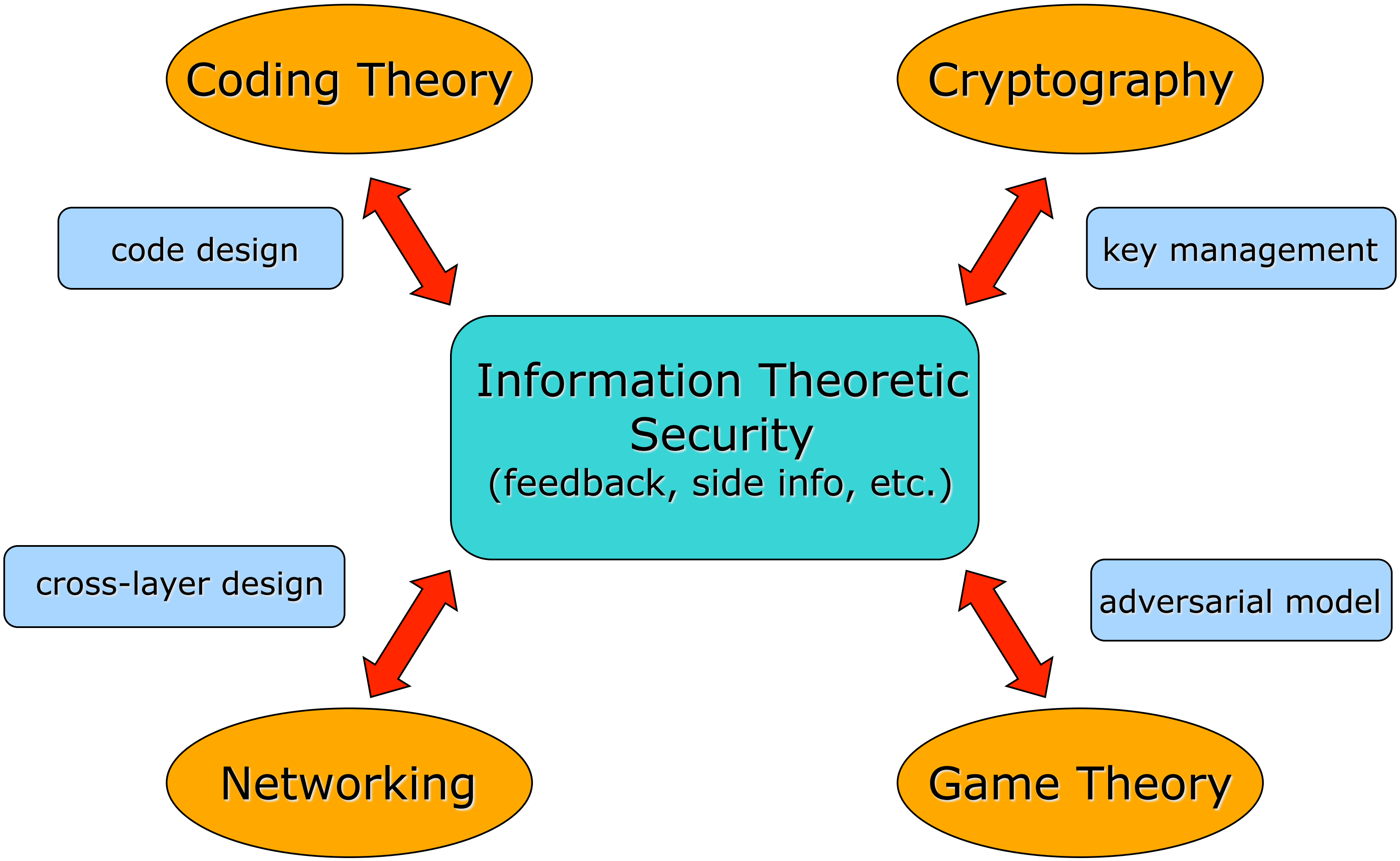
- <u>Interference Channel</u> [w/ Liang, Someck-Baruch, Shamai, Verdú - IT'09 (cognitive) & w/ Koyluoglu, El Gamal, Lai - IT'11 (interference alignment)]:



- <u>Relay Channels</u> [e.g., w/ Aggarwal, Sankar, Calderbank – JWCN'09 & w/ Kim – IT'11]: Source and relay cooperate to improve security.

- <u>MIMO</u> [e.g., w/ Liu, Liu, Shamai – IT'10]: Use of multiple transmit & receive antennas allows simultaneous secure broadcast <u>without rate penalty</u>.

A Rich Area



Liang, Poor & Shamai, *Information Theoretic Security* (Now '09)
Liu & Trappe, Eds., *Securing Wireless Communications at the Physical Layer* (Springer '10)
Bloch & Barros, *Physical Layer Security* (CUP '11)

Distributed Learning
Inference in Wireless Sensor Networks

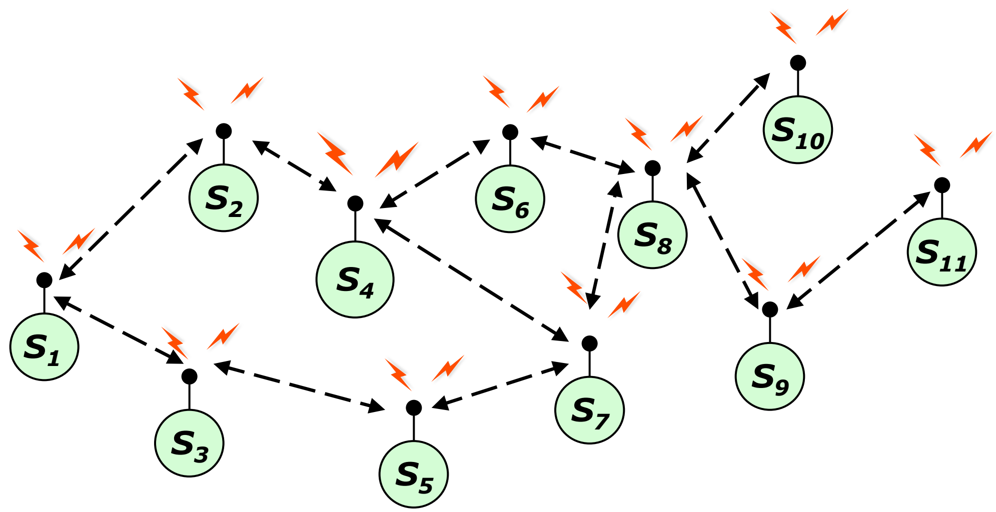
[Joint work with Joel Predd, Sanjeev Kulkarni, et al.]

Sensor Field

Distributed Learning

A Model for Dist'd Learning in WSNs

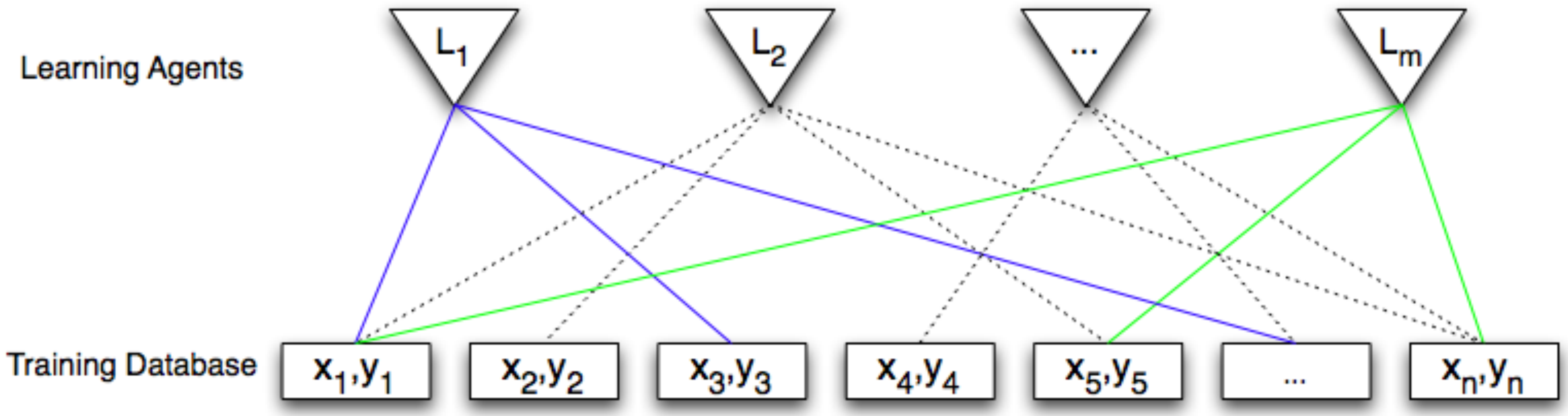
"A distributed sampling device with a wireless interface"



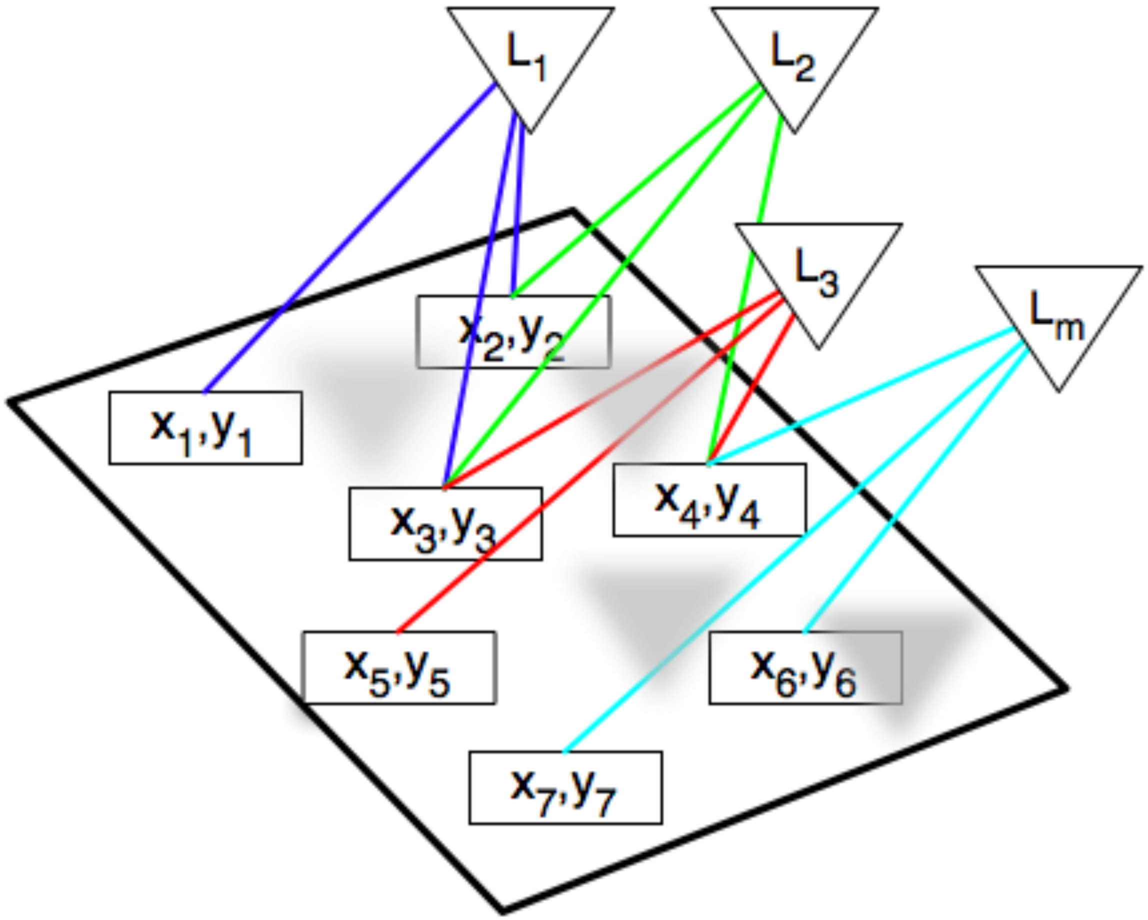
- Each sensor measures a subset of a large data set
- Each sensor can access all neighboring sensors' measured data.

A General Model

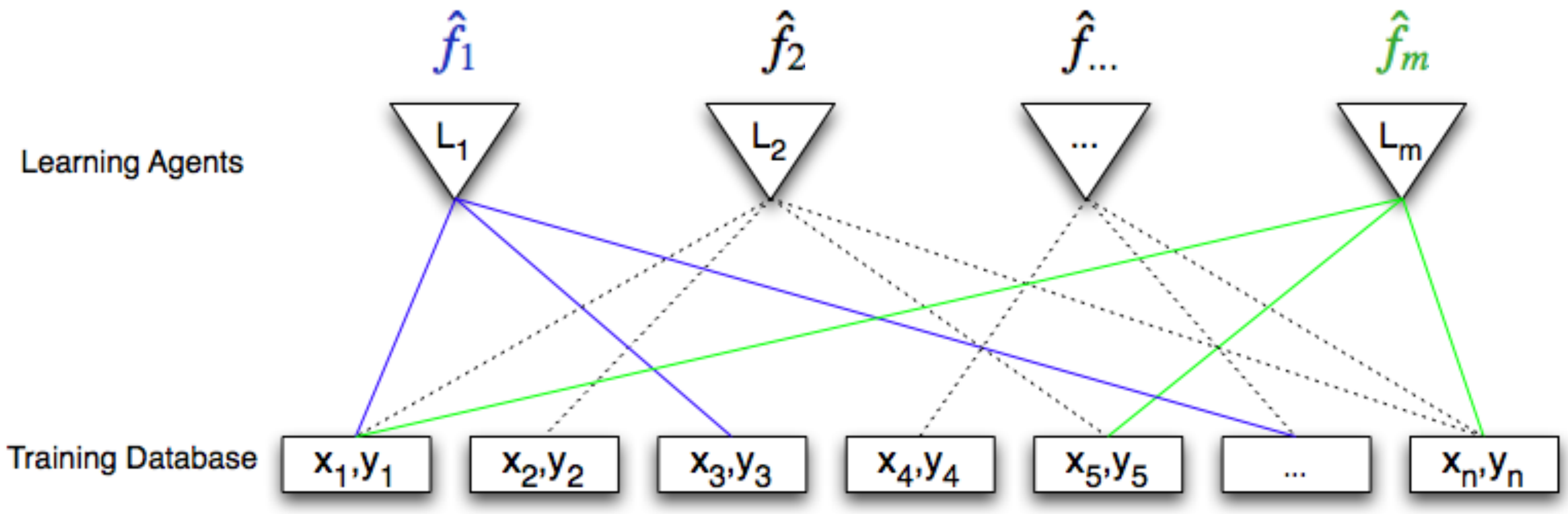
- *m learning agents (i.e., sensors)*
- *n training data* $S = \{(\mathbf{x}_i, y_i)\}_{i=1}^{n}$



Example:
Spatio-Temporal Field Estimation



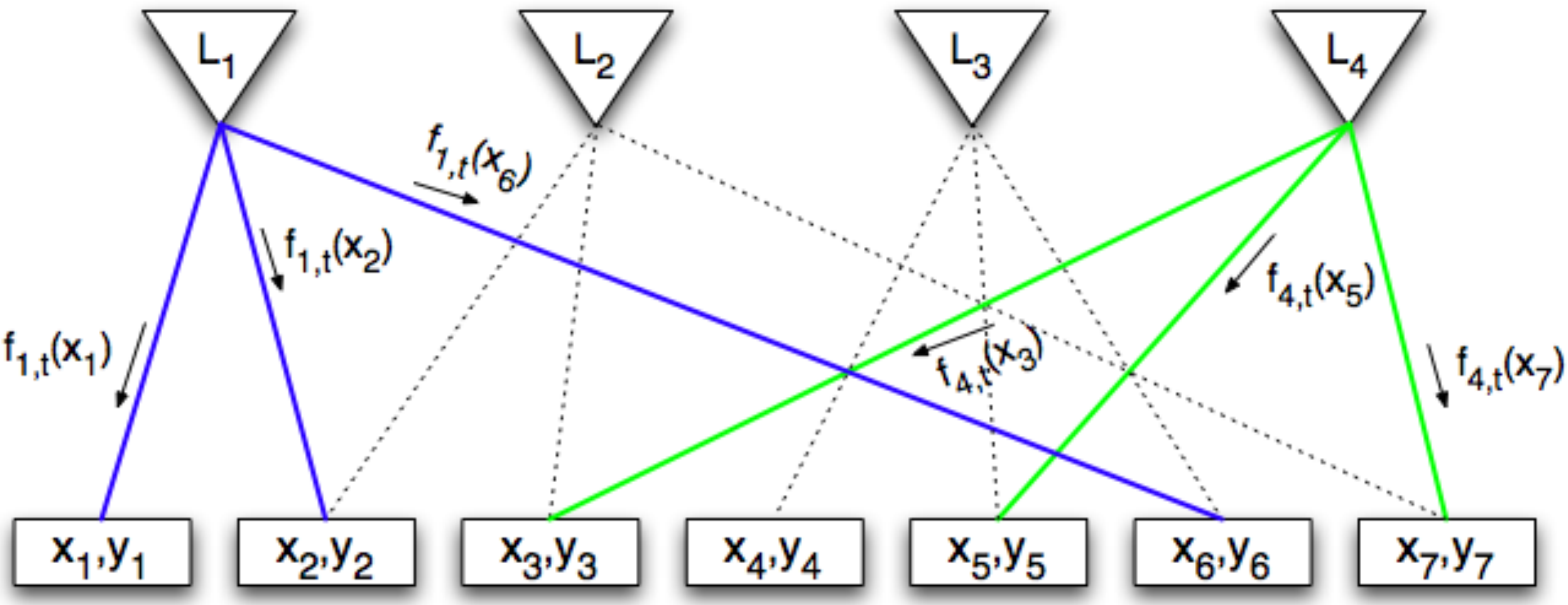
"Local" Learning: A Natural Approach



- Each learns the field with its locally available data.
- This is generally locally incoherent – e.g., $\hat{f}_1(\mathbf{x}_1) \neq \hat{f}_m(\mathbf{x}_1)$

A Collaborative Algorithm

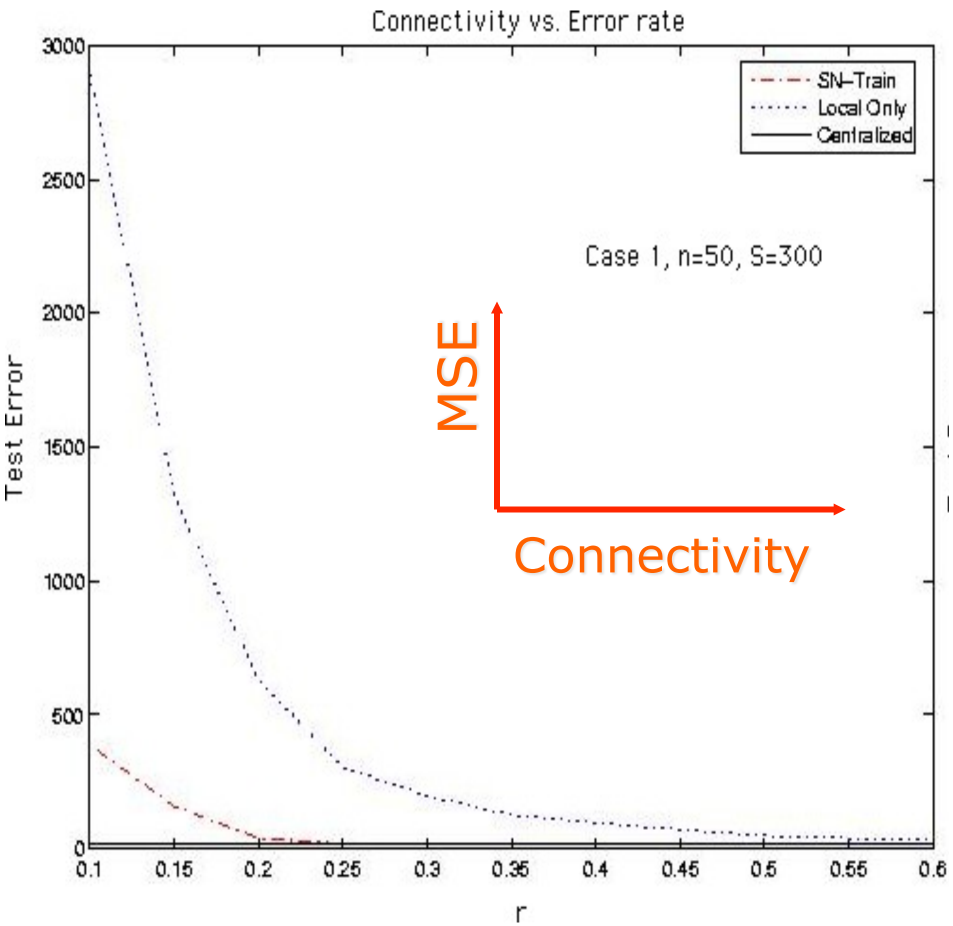
[w/ Predd, Kulkarni, IT'09]



- Message passing is used to update the database.
- Nice properties & combines coherence with locality.

Experiment

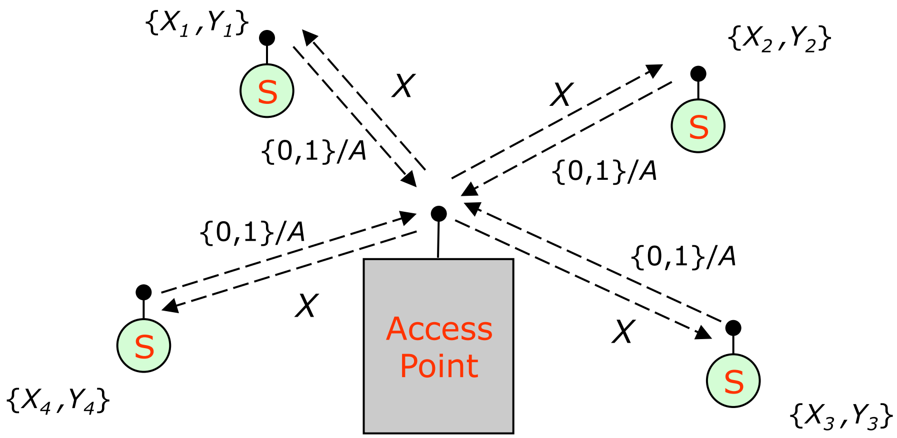
- 50 sensors uniform in [-1, 1]
- Sensor *i* observes $y_i = f(x_i) + n_i$
  - $\{n_i\}$ is i.i.d. $N(0,1)$
  - regression function *f* is linear
  - *i* and *j* are neighbors: $|x_i - x_j| < r$
- Sensors employ linear kernel



Related Results

- <u>Consistency w. Limited Capacity</u>

  [w/ Predd, Kulkarni - IT'06]



- <u>Judgment Aggregation</u>

  [w/ Osherson et al. - *Decision Analysis* '08, '11]

- <u>Attribute Distributed Data</u>

  [w/ Zheng et al. – SP'11]

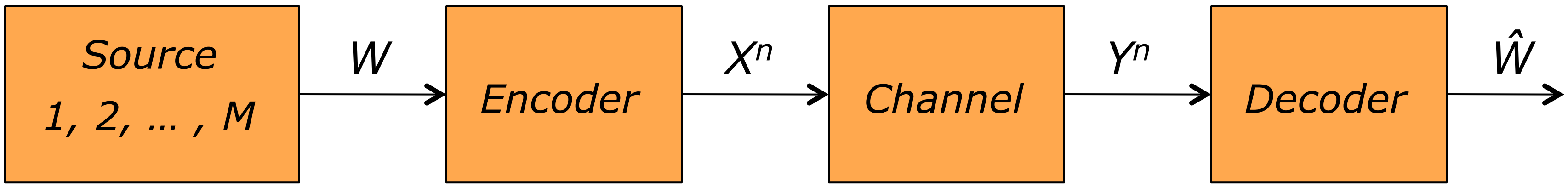
Finite-Blocklength Capacity

Multimedia Information Transmission

[Joint work with Yury Polyanskiy & Sergio Verdú]

Information & Inference in the Wireless PHY

A Fundamental Problem



- *(n,M,ε) code*: $P(W \neq \hat{W}) \leq \varepsilon$
- *Fundamental limit*: $M^*(n,\varepsilon) = \max\{M: \exists \text{ an } (n,M,\varepsilon) \text{ code}\}$
- *Shannon*: As $n \to \infty$, $\varepsilon \to 0$

$$\frac{\log M^*(n,\varepsilon)}{n} \to C \quad \text{(capacity)}$$

- *In many apps (e.g., multimedia) n and ε are noticeably finite.*

Finite n and ε

[w/ Polyanskiy, Verdú, IT'10 & IT'11]

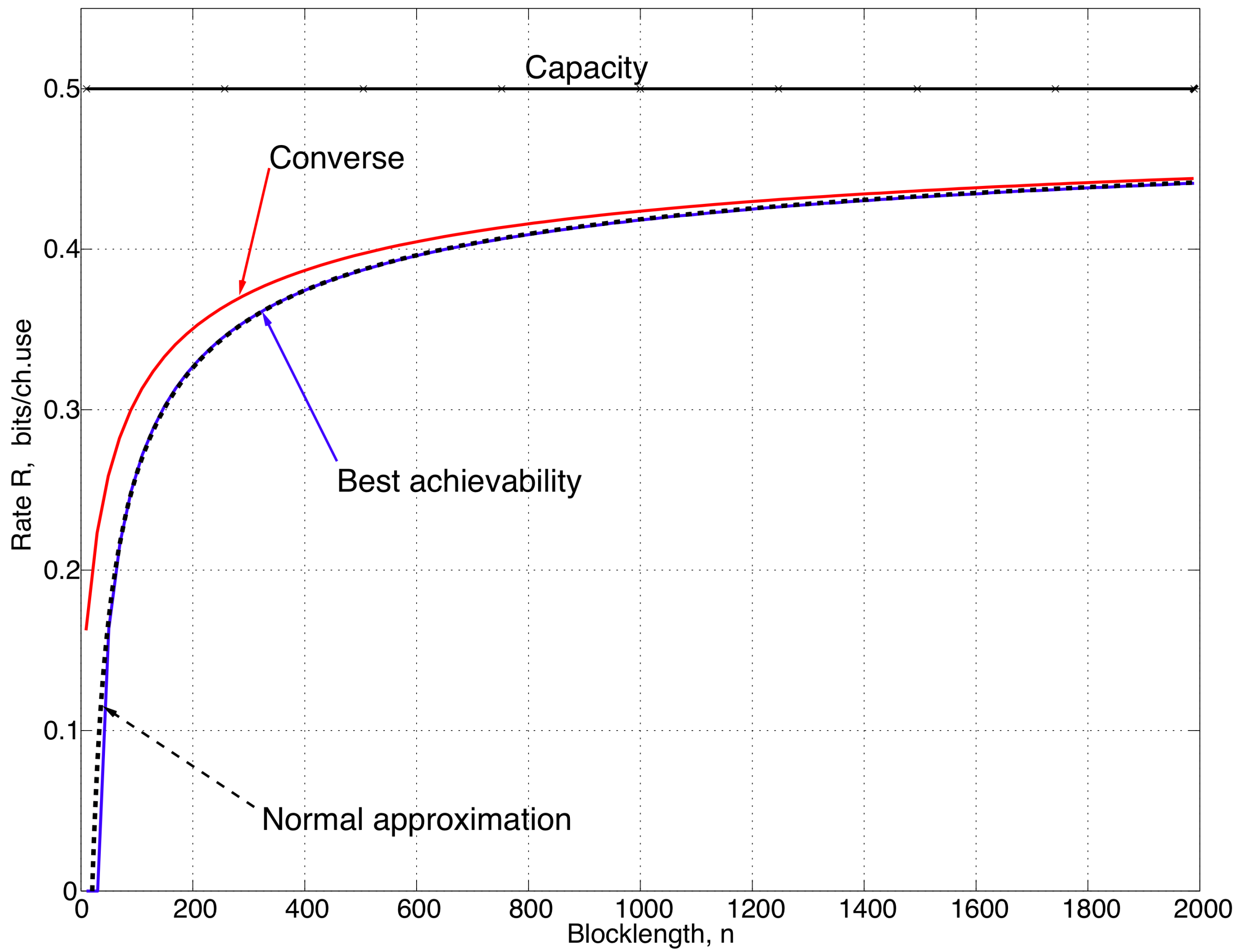
- *Bounds:*
  - *Shannon-Feinstein (1954/57); Gallager (1965)*
  - *Random coding union (2008); dependence testing (2008)*
- *Approximation:*
  - *Strassen (1962) – discrete memoryless channels*
  - *New bounds yield (2008/09) – sharper for DMCs; Gaussian; fading*

$$\log M^*(n,\varepsilon) = n\,C - \sqrt{nV}\,Q^{-1}(\varepsilon) + O(\log n)$$

$V = \mathrm{Var}[i(X^*,Y^*)]$ ("*dispersion*")

Finite-Blocklength Capacity

Ex: AWGN (SNR = 0 dB; $\varepsilon = 10^{-3}$)

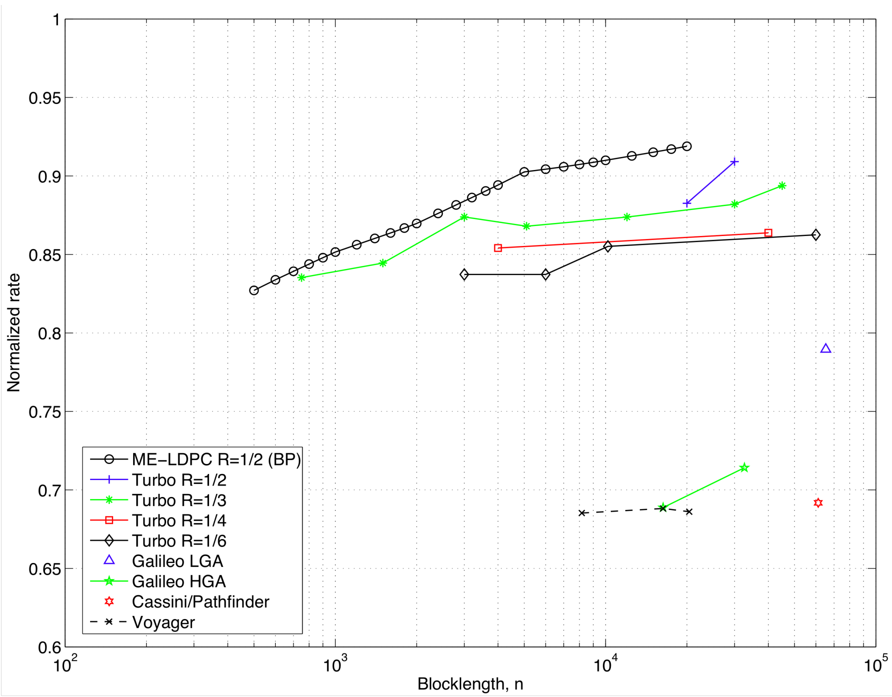


Finite-Blocklength Capacity

Some Applications

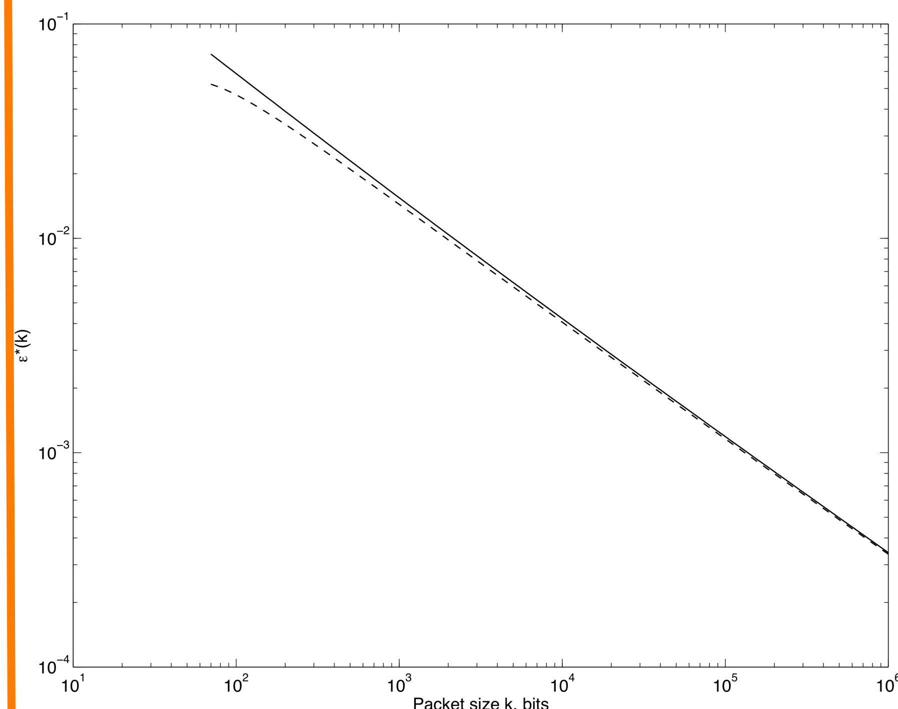
Analysis of Codes

(normalized to the approx.; ε = 10^{-4})



ARQ: Optimal ε vs. *n*

(AWGN; SNR = 0 dB)



More generally: information theory for finite *n*?

Finite-Blocklength Capacity

Message Delivery in Small World Networks

Social Networking (Information & Inference)

[Joint work with Hazer Inaltekin & Mung Chiang]

Message Delivery in Small World Social Networks

- Milgram's 1967 experiment:

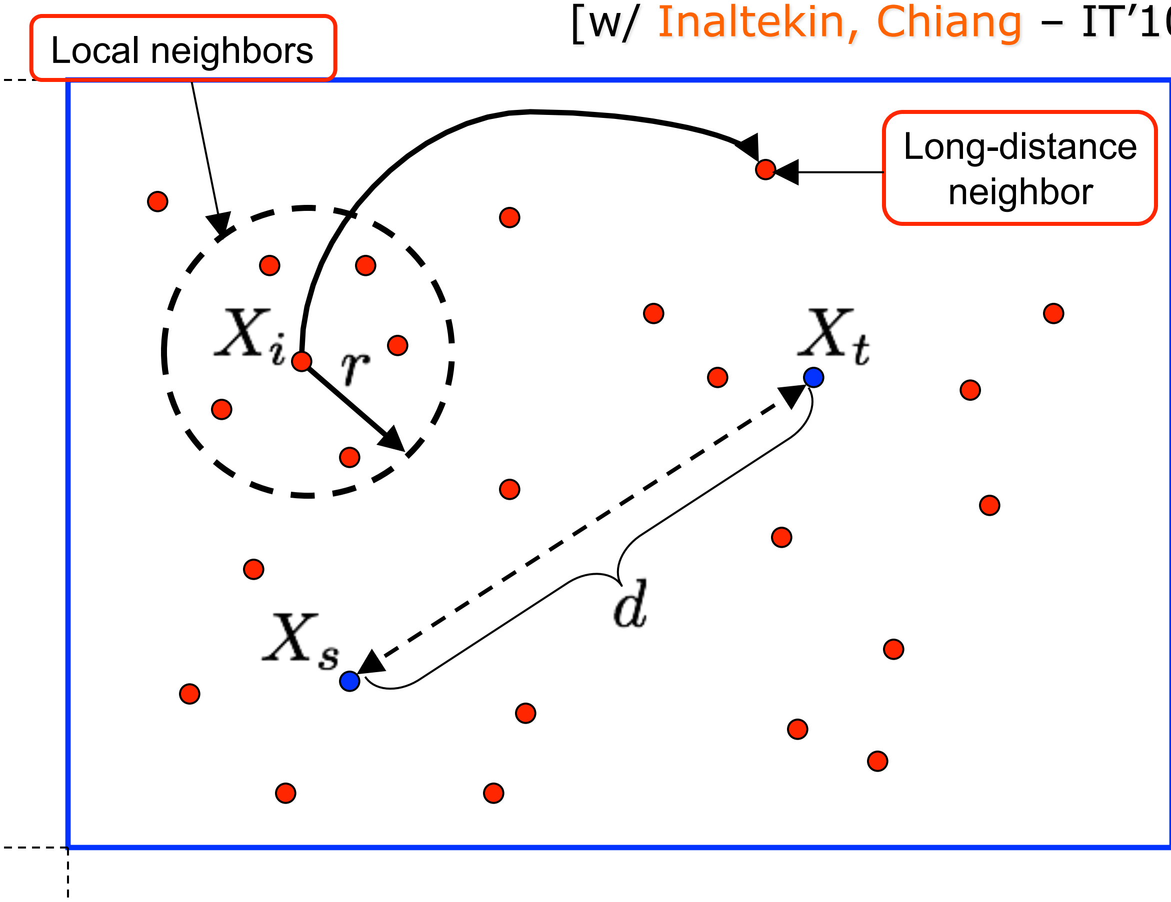
$$\text{“ } \mathbb{E}[\text{ Path Length }] = 6. \text{”}$$

  - Two striking conclusions:
    - people are connected through short chains of acquaintances
    - these chains can be found via local information

- Analysis can help explain this

Random Geographic Graph Model

[w/ Inaltekin, Chiang – IT'10]



- Source and target nodes are placed at arbitrary positions.
- Their separation is *d*.
- *n* other relay nodes are distributed uniformly over the domain.
- Each node has local communication range *r*.
- Each node has one long-distance neighbor.
- Greedy geographic routing.

E.g.:

- Social networks: Granovetter, *Am. J. Sociology*'78
- Ad hoc networks:Reznik, Kulkarni, Verdú, *Comm. Inf. Syst.*'04

Average Message Delivery Time, g(d), in the Continuum Limit ($n \to \infty$)

- Define

$$g_0 = g(0), g_1 = g(d) \text{ for } 0 < d < r,$$

$$g_k = g(d) \text{ for } (k-1)r \le d < kr.$$

- Recursive equation:

$$g_{k+1} = 1 + \left(1 - \alpha\,(k-1)^2\right) g_k + \alpha \sum_{i=1}^{k-1} (2i-1)\, g_i$$

$$\alpha = \frac{\pi r^2}{R^2 - \pi r^2}$$

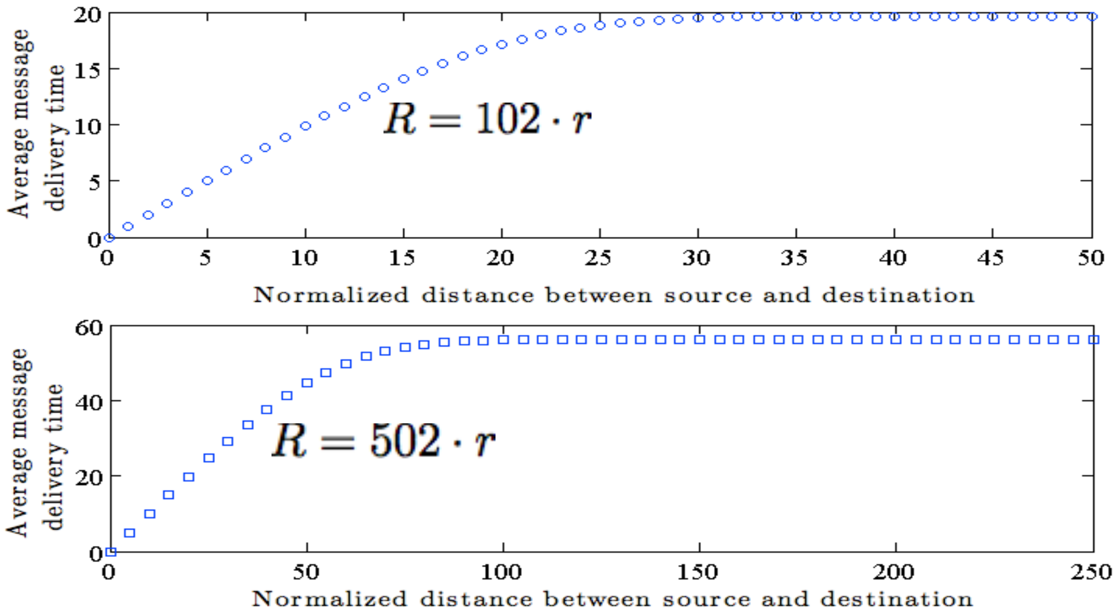
R = domain dimension

- Solution for the recursion:

$$g_{k+1} = 1 + \sum_{j=1}^{k} \prod_{i=1}^{j} \beta_i \text{ for } k \ge 1.$$

$$\beta_k = 1 - \alpha(k-1)^2$$

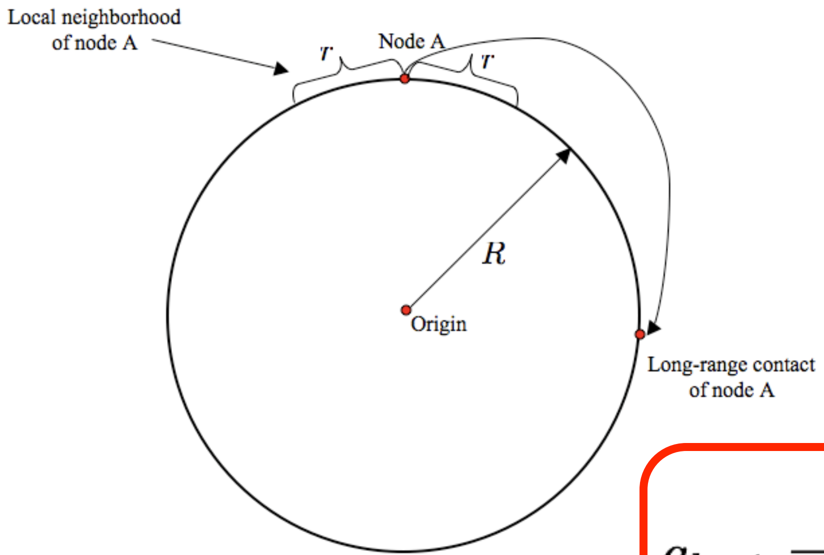
Numerical Examples: Average Message Delivery Time



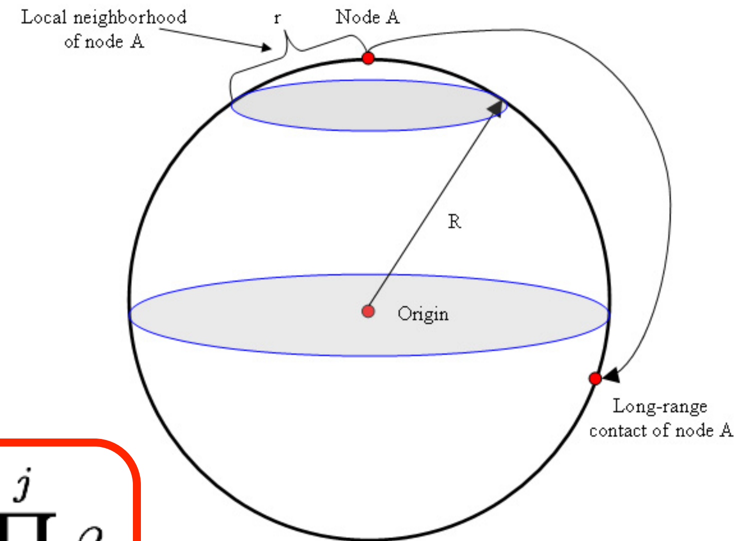
- Effects of Short-cuts on Packet Delay:
  - short distances: message delivery grows linearly
  - long distances: message delivery time saturates to a constant
  - Observation of Travers & Milgram [*Sociometry* '69]: "Chains which converge on the target principally by using geographic information reach his hometown or surrounding areas readily, but once there often circulate before entering target's circle of acquaintances."

Other Network Topologies

On the Circle



On the Sphere



$$g_{k+1} = 1 + \sum_{j=1}^{k} \prod_{i=1}^{j} \beta_i$$

$$\beta_i = \frac{\pi - i\theta}{\pi - \theta}$$

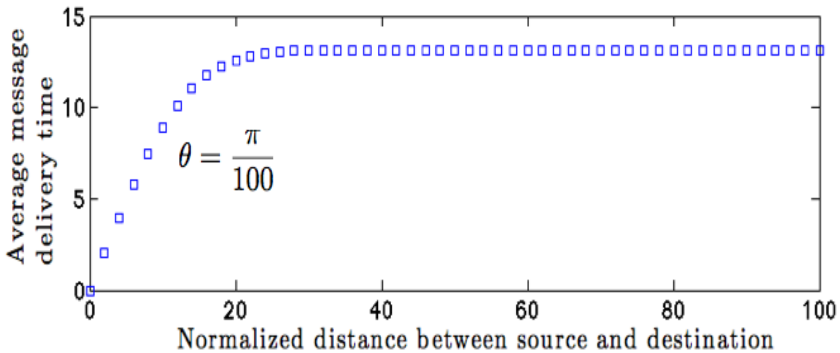
$$\theta = \frac{r}{R}$$

$$\beta_i = \frac{\cos(\theta) + \cos((i-1)\theta)}{1 + \cos(\theta)}$$

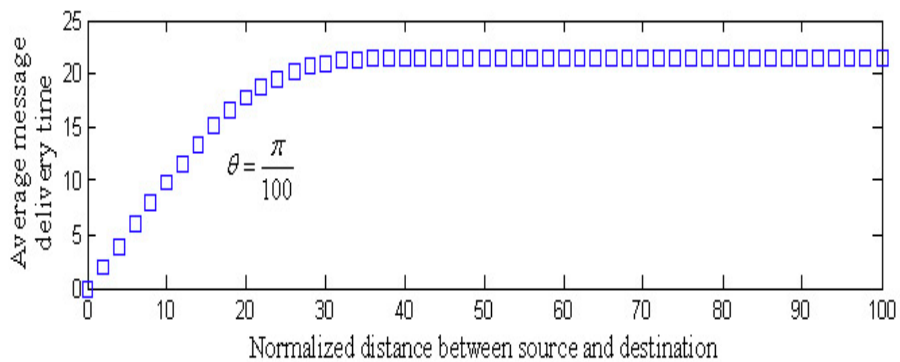
$$\theta = \frac{r}{R}$$

Numerical Examples: Other Network Topologies

On the Circle



On the Sphere

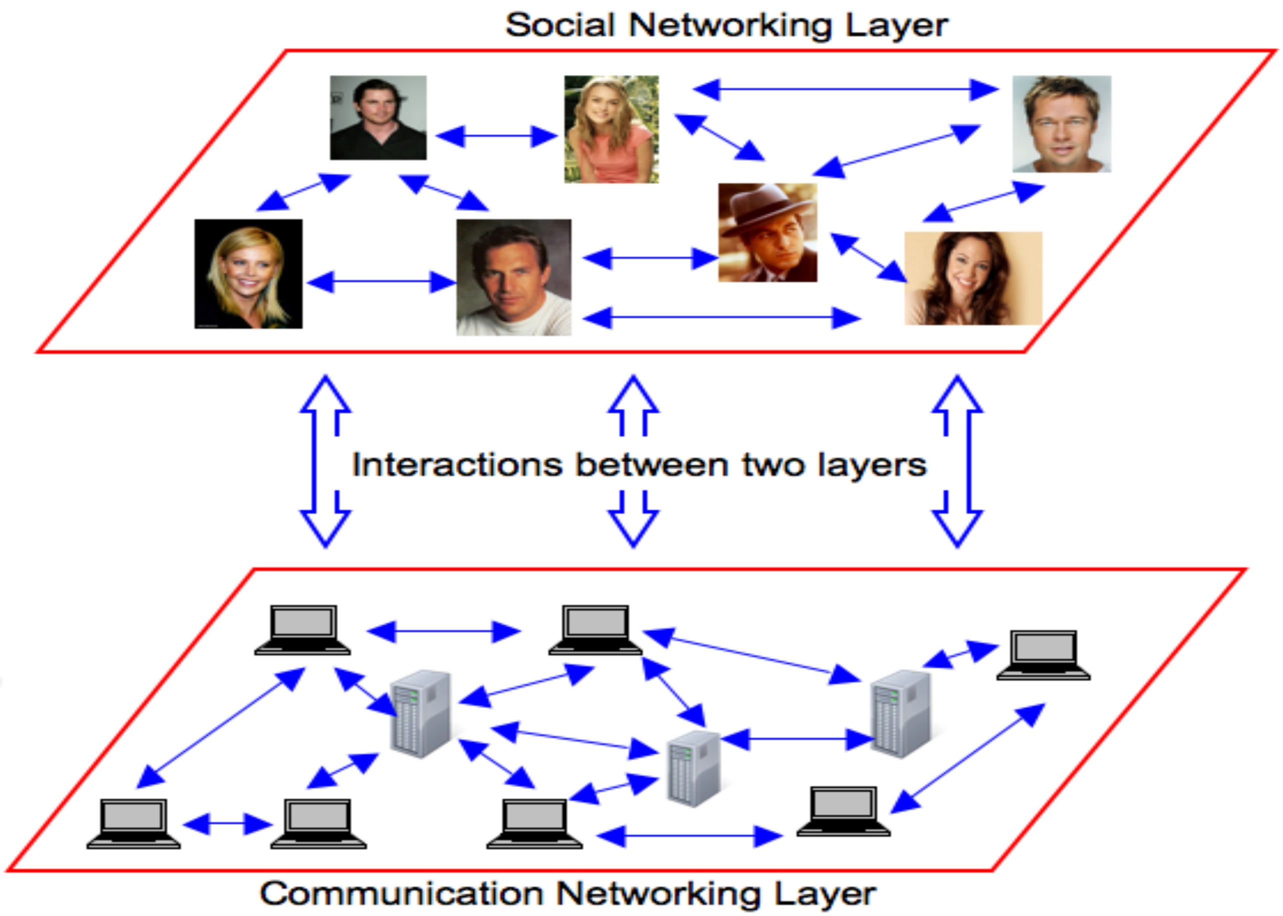


Generalization to other topologies, other connection models, etc.: [w/ Inaltekin, Chiang – IT'10 & J. Math. Soc., to appear]

Social Overlay/Communication Underlay

virtual:

physical:



Social overlay imposes new structure (e.g., trust).

Summary: Four Problems in the Wireless PHY Motivated by the APP

- *PHY Security in Wireless Communication Networks*

  Motivated by Secure Information Transmission

- *Distributed Learning*

  Motivated by Statistical Inference in Wireless Sensor Networks

- *Finite-Blocklength Capacity*

  Motivated by Multimedia Information Transmission

- *Message Delivery in Small-World Networks*

  Motivated by Social Networking (Information & Inference)

Thank you!