MIT LIDS
November 14, 2009

Networks and Information
Paths Ahead

Vince Poor
(poor@princeton.edu)

Overview

- *Issues Raised by JNT:*
  - *Theory/methodology "push"*
  - *Problem/applications "pull"*
  - *Bridging opportunities*
- *My talk: Address these by example*
- *No big philosophical ideas, but some messages:*
  - *Analysis still matters*
  - *The past is important*
  - *The set of bridging opportunities is broad*

So, Three Examples (Very Briefly)

Pull: Security in Wireless Networks

- *Push: Information Theoretic Security*

Pull: Multimedia Communications

- *Push: Finite-Blocklength Capacity*

Pull: Social Networking

- *Push: Small-World Networks*

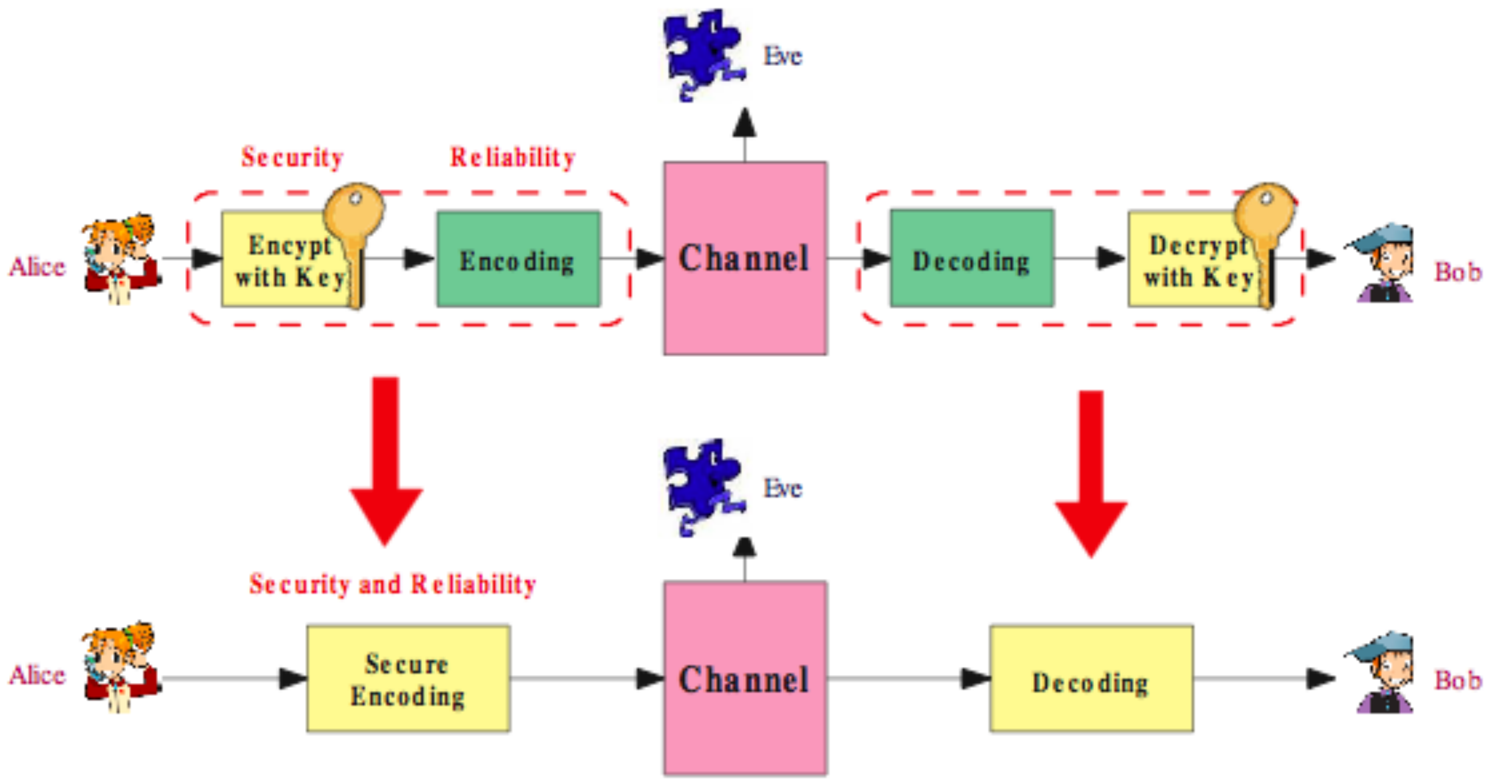
SECURITY IN WIRELESS NETWORKS

Information Theoretic Security

Exploiting the Wireless PHY

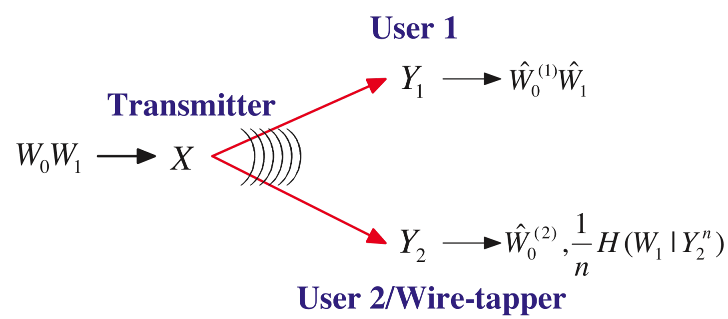
- Key Techniques for Improving Capacity & Reliability:
  - *MIMO, Cooperation & Relaying*
  - *Cognitive Radio*
- What About Security?
  - *Traditionally a higher-layer issue*
  - *Encryption can be complex and difficult without infrastructure*
  - *Information theoretic security examines the fundamental ability of the PHY to provide security*
  - *Origins: Shannon (1949) & Wyner (1975) provided the tools*
  - *Today: Application to wireless networking models*

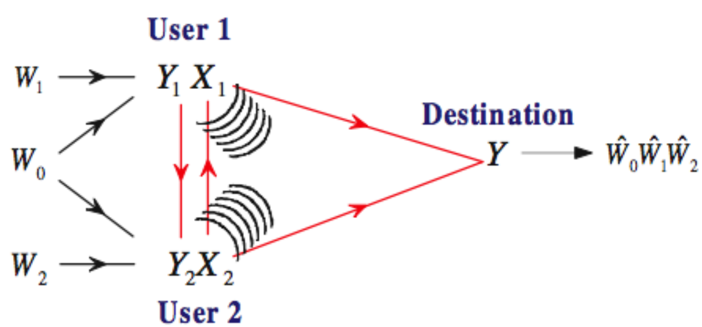
Physical Layer Security
Joint Encoding for Security and Reliability



Building Blocks
Secrecy Capacity Regions

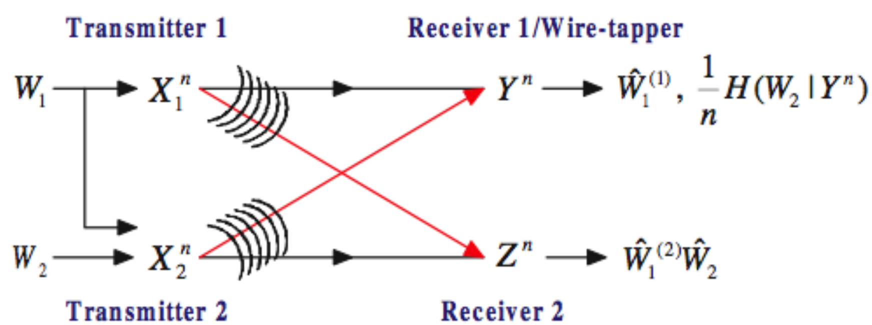
Broadcast Channel:



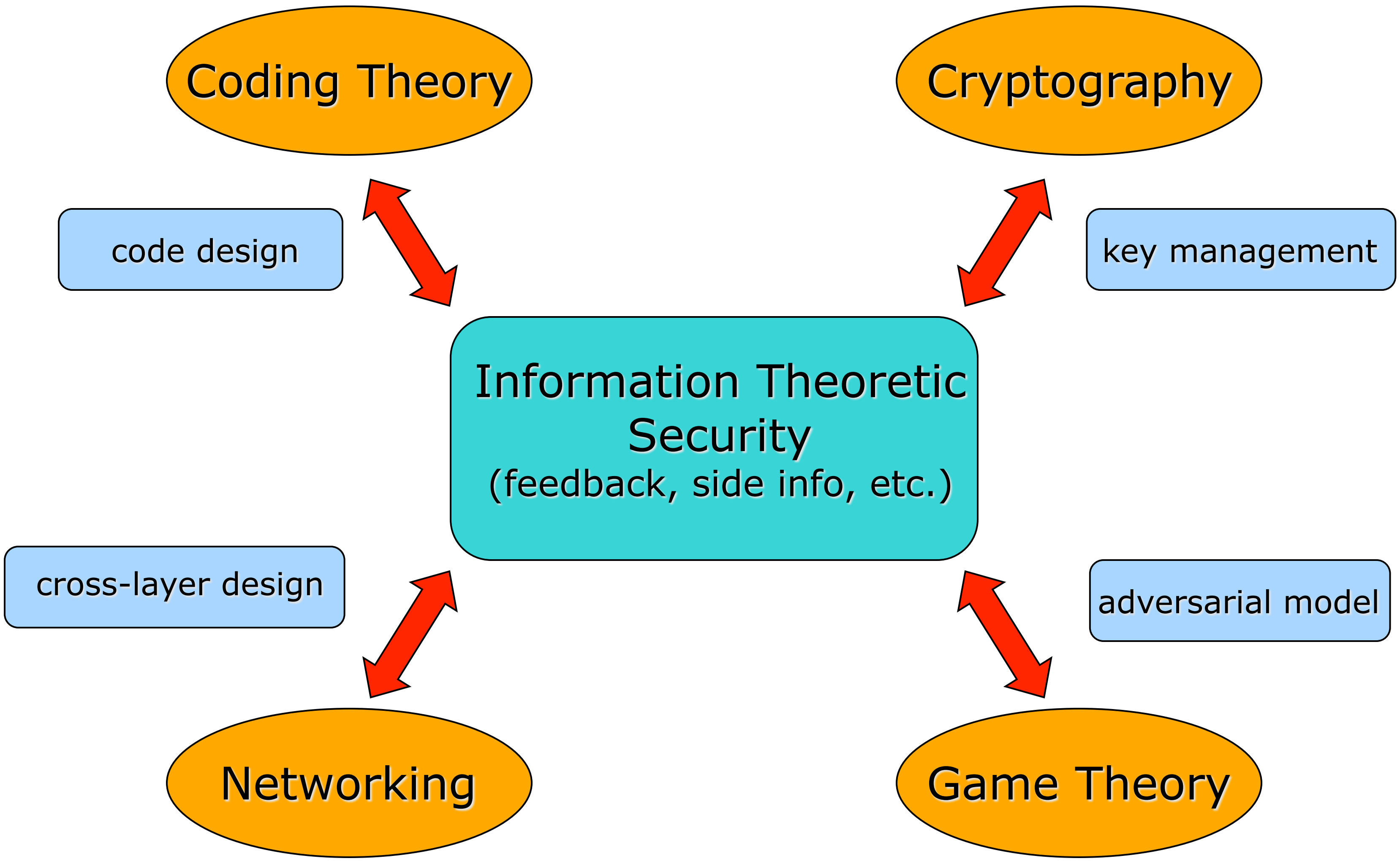


:Multiple-access Channel

Interference Channel:



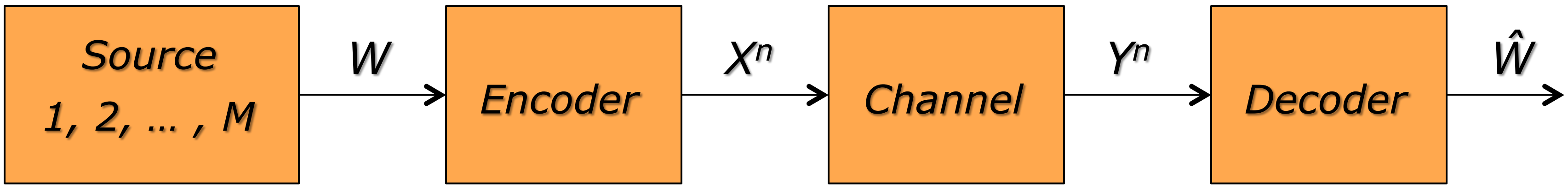
A Rich Area for Bridging



MULTIMEDIA COMMUNICATIONS

Finite-Blocklength Capacity

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 $n \longrightarrow \infty$, $\varepsilon \longrightarrow 0$

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

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

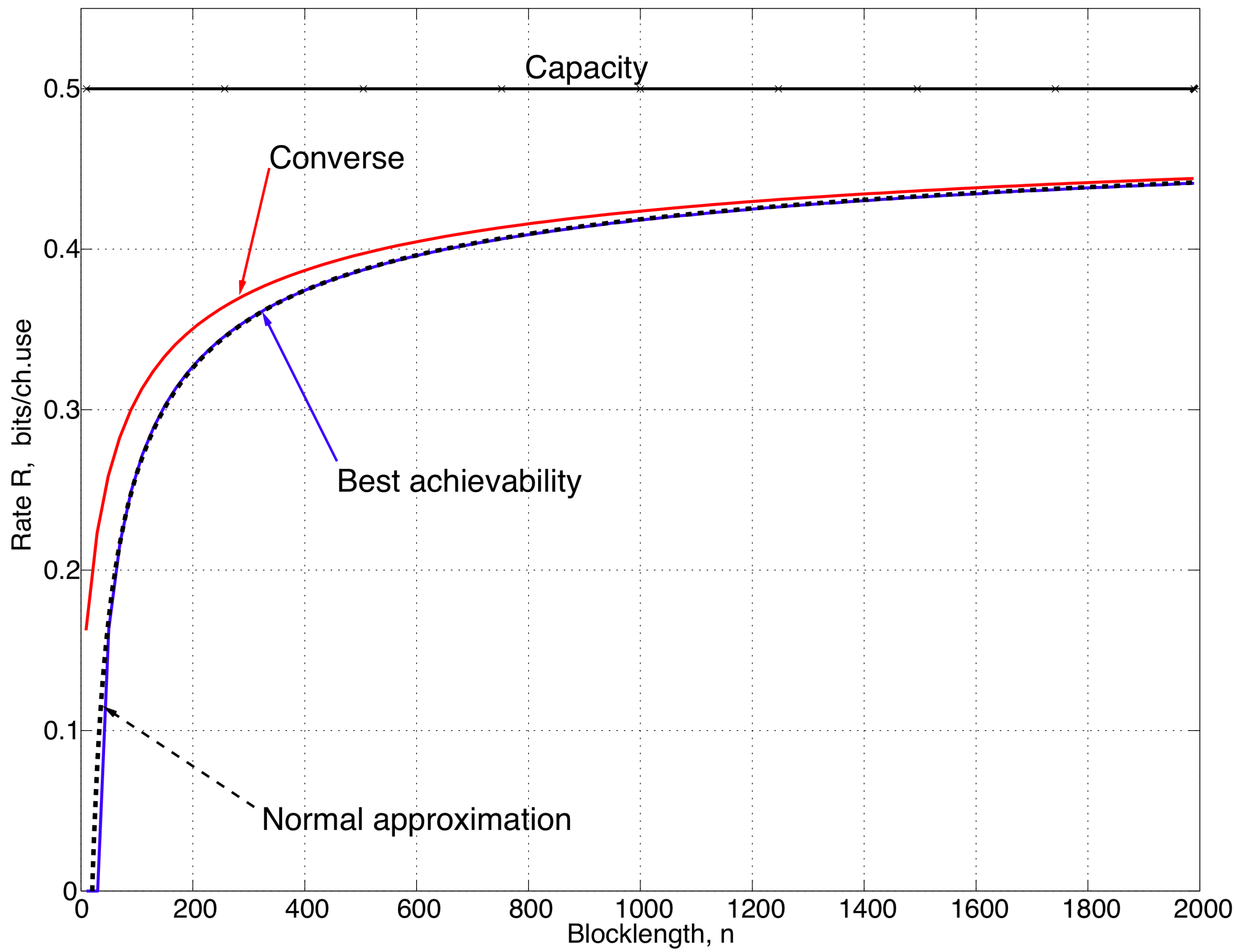
Finite n and ε

- *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*

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

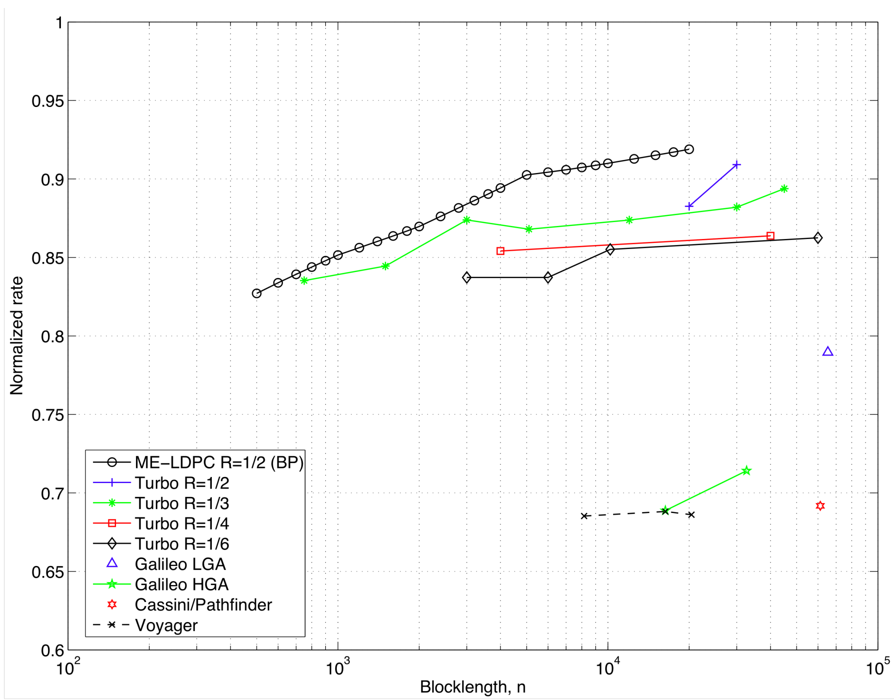
$V = \mathrm{Var}[i(X^*,Y^*)]$ (*"dispersion"*)

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

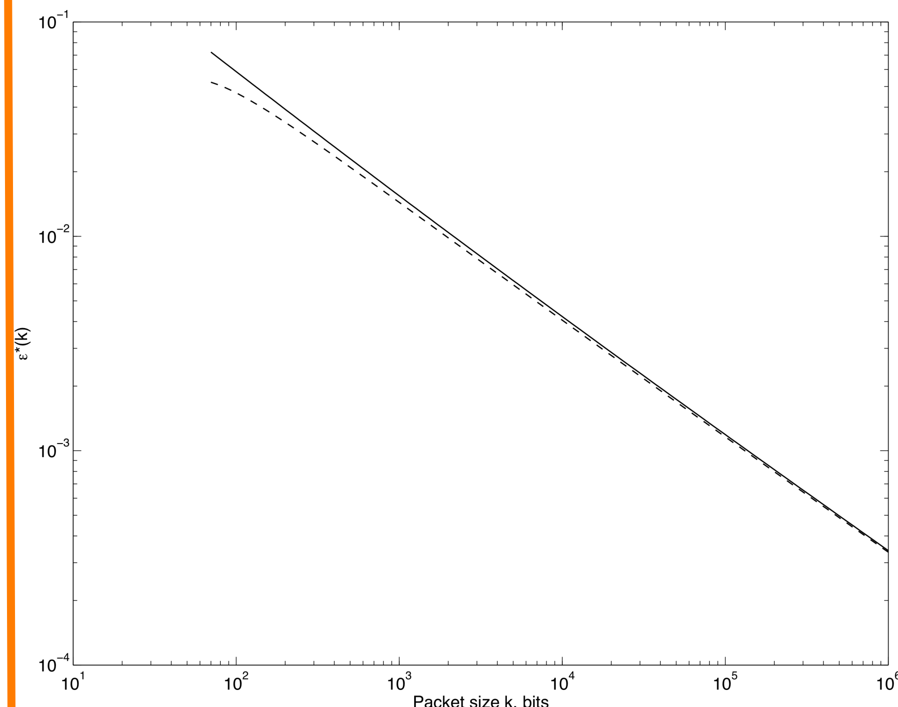


Bridges
(Not Very Long Ones)

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*?

Networks and Information: Paths Ahead

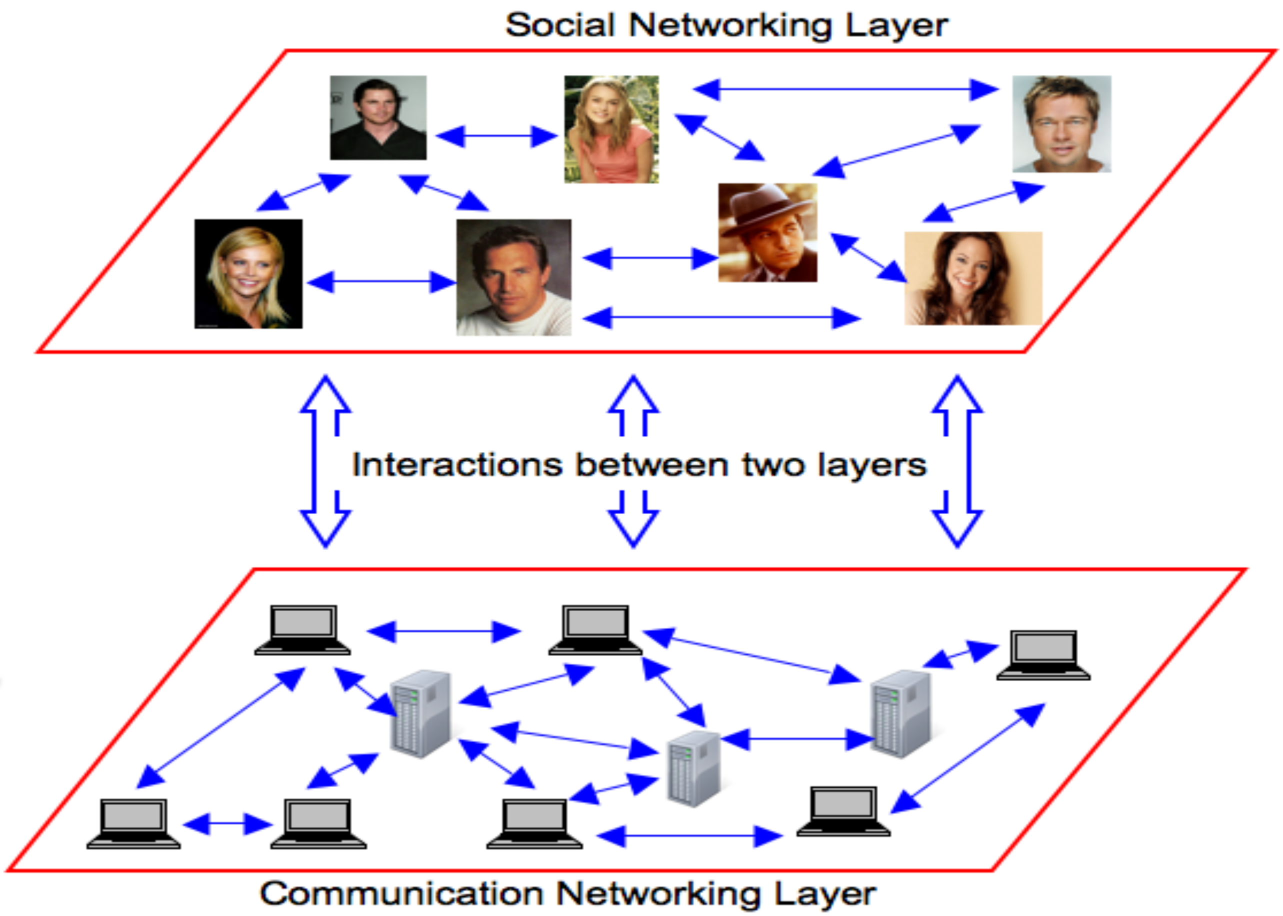
SOCIAL NETWORKING

Small-World Networks

Social Overlay/Communication Underlay

virtual:

physical:



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

Message Delivery in Small World Social Networks

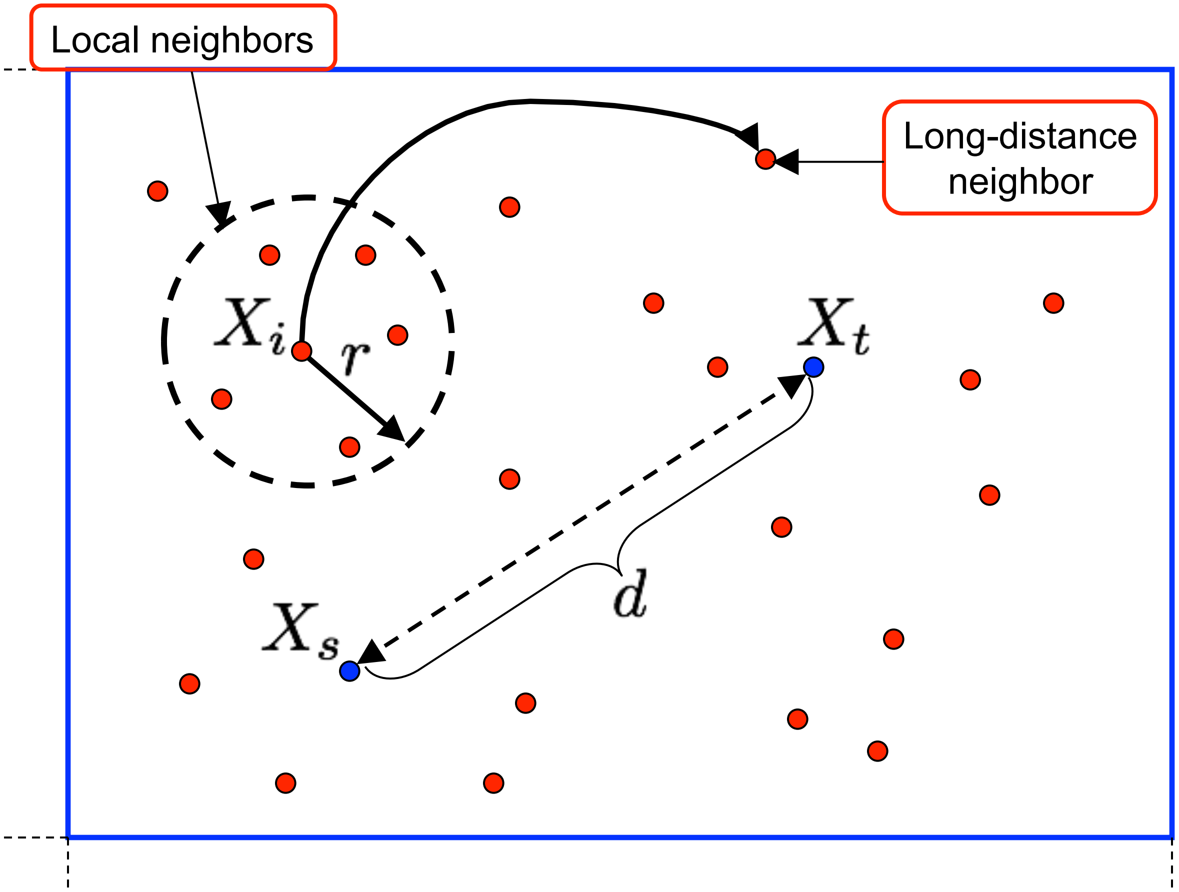
- Milgram's 1967 experiment:

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

  - 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



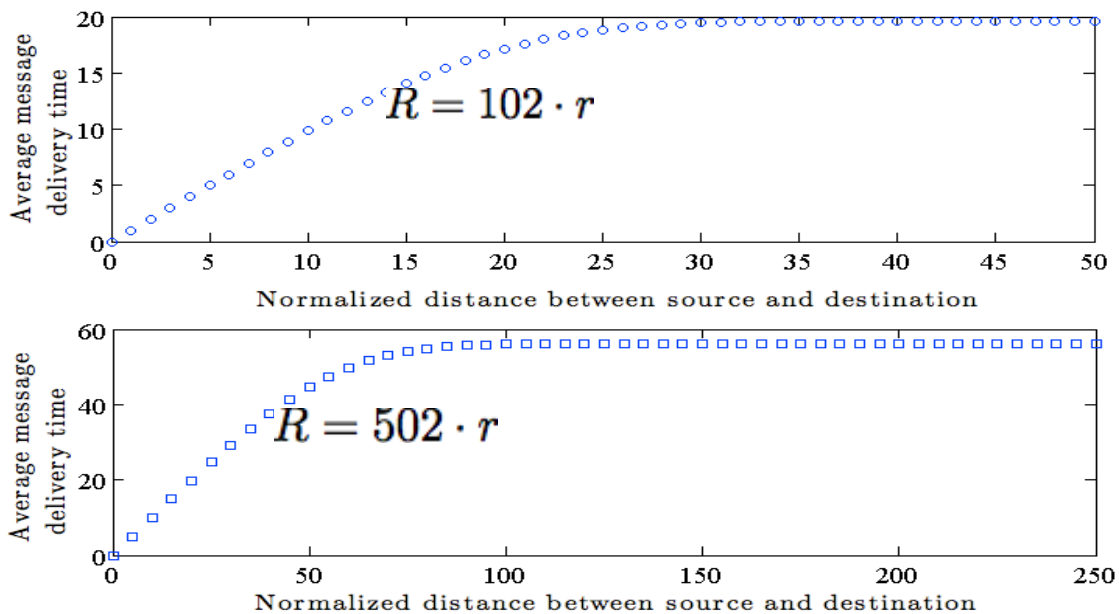
- Source and target nodes are placed at arbitrary positions.
- *n* other relay nodes are distributed uniformly over the domain.
- Each node has local communication range *r*.
- Each node has one long-distance neighbor.
- Greedy geographic routing.

E.g.:

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

Average Message Delivery Time

- Can get closed form in the continuum limit:



- Effects of Short-cuts on Packet Delay:
  - short distances: message delivery grows linearly
  - long distances: message delivery time saturates to a constant
  - agrees with experimental observations of Travers & Milgram [*Sociometry'*69]
  - similar results for other network topologies (circle, sphere, etc.)

Bridging (It's Not All About CS & Biology)

Psychology

- *Political polling/judgment aggregation*

Sociology

- *Spread of HIV*

Politics

- *Foreign policy analysis*

Thank You!