Fundamental Limits
on
Information Security and Privacy

Vince Poor
(poor@princeton.edu)

.

Overview

Two topics:

- Secrecy in wireless data transmission
- Privacy of information sources, with applications in smart grid

Common theme:

- Information theoretic characterization of fundamental limits

Outline

1. Physical Layer Security in Wireless Networks

2. Privacy-Utility Tradeoffs, with Applications in Smart Grid

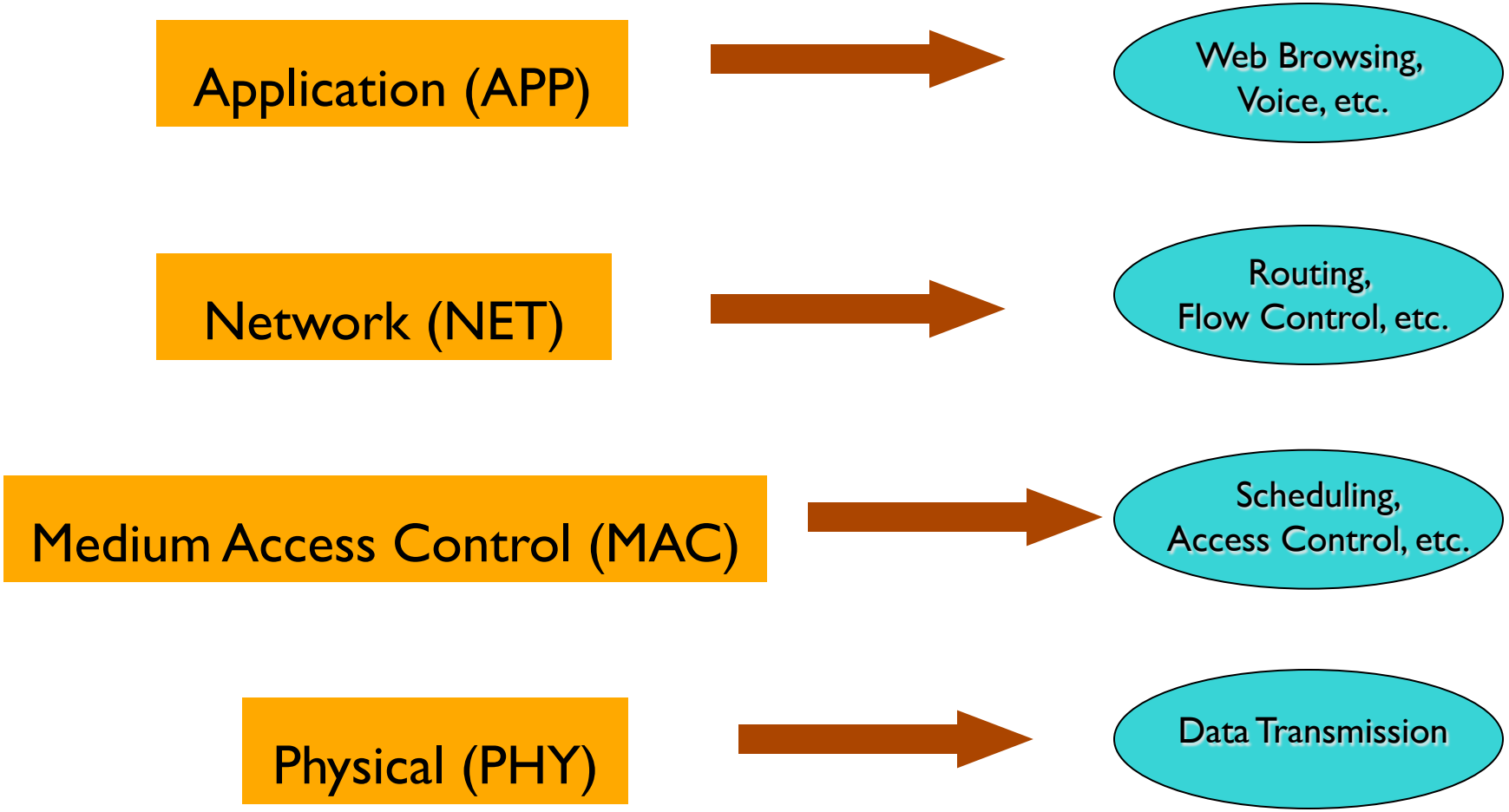
3. Summary

Physical Layer Security

in

Wireless Networks

Wireless Networks: Layers



Motivation: Exploiting the Physical Layer

- Key Techniques for Improving Capacity & Reliability:
  - MIMO (Multiple-Antenna Systems)
  - Cooperation & Relaying
  - Cognitive Radio

Motivation: Exploiting the Physical Layer

- Key Techniques for Improving Capacity & Reliability:
  - MIMO (Multiple-Antenna Systems)
  - Cooperation & Relaying
  - Cognitive Radio
- What About Security?
  - Traditionally a higher-layer issue (e.g., APP)
  - Encryption can be complex and difficult without infrastructure
  - Information theoretic security examines the fundamental ability of the PHY to provide security (confidentiality)

Information Theoretic Secrecy:
Shannon's Model

Shannon [1949]: For cipher, perfect secrecy requires a one-time pad.

[I.e., the entropy of the key must be at least the entropy of the source: $H(K) \geq H(M)$]

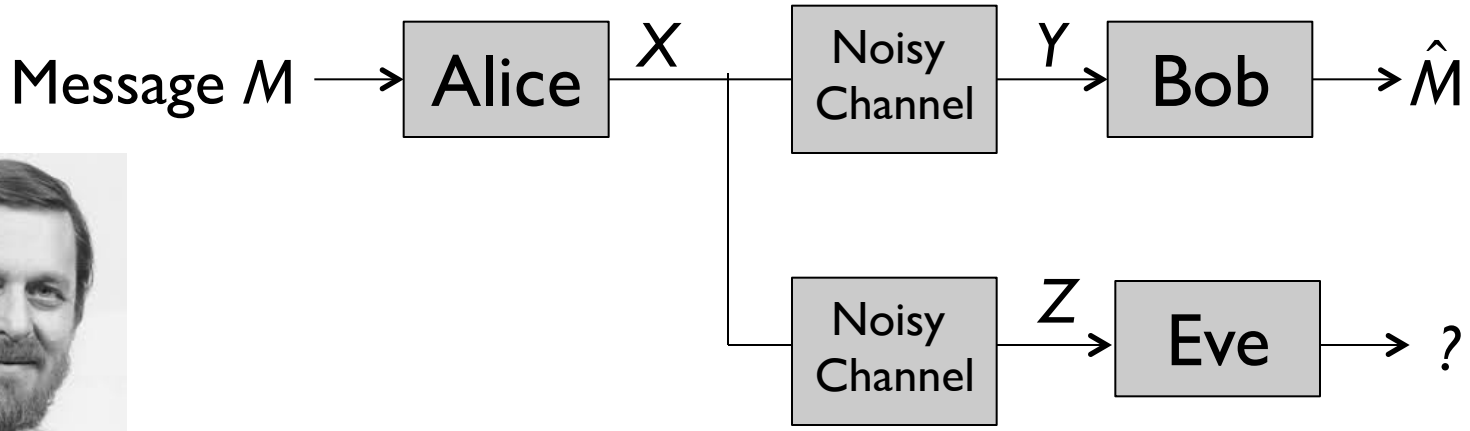
SIGSALY vs. Enigma

one-time pad

not a one-time pad

Information Theoretic Secrecy:
Wyner's Model

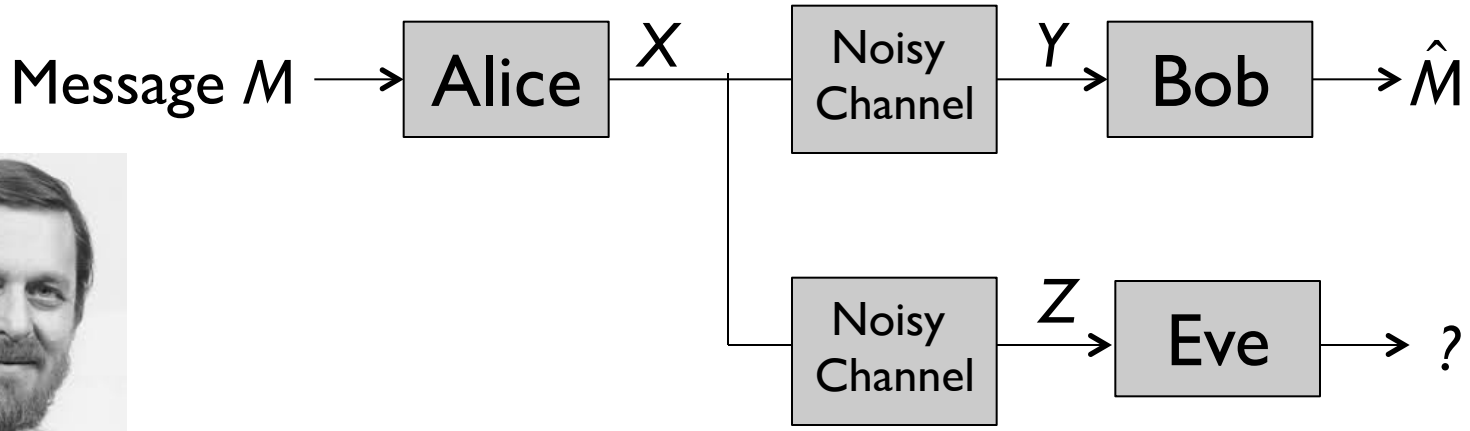
"The Wiretap Channel"



- Tradeoff: reliable rate R to Bob vs. the "equivocation" $H(M|Z)$ at Eve

Information Theoretic Secrecy:
Wyner's Model

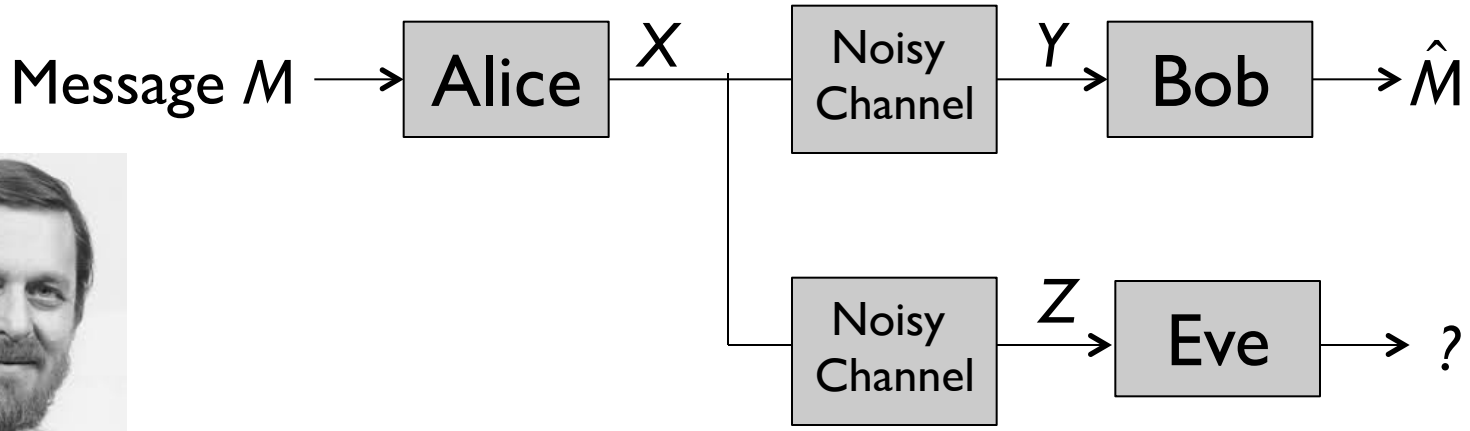
"The Wiretap Channel"



- Tradeoff: reliable rate R to Bob vs. the "equivocation" $H(M|Z)$ at Eve
- Secrecy capacity = maximum R such that $R = H(M|Z)$

Information Theoretic Secrecy:
Wyner's Model

"The Wiretap Channel"



- Tradeoff: reliable rate R to Bob vs. the "equivocation" $H(M|Z)$ at Eve
- Secrecy capacity = maximum R such that $R = H(M|Z)$
- Wyner [1975]: Secrecy capacity > 0 iff. Z is degraded relative to Y

Physical Layer Security in Wireless Networks

- There has been a resurgence of interest in Wyner's ideas, as encryption is impractical for emerging wireless networking paradigms.

Physical Layer Security in Wireless Networks

- There has been a resurgence of interest in Wyner's ideas, as encryption is impractical for emerging wireless networking paradigms.

- The physical properties of radio propagation (diffusion & superposition) provide opportunities for this, via

  - fading: provides natural degradedness over time
  - interference: allows active countermeasures to eavesdropping
  - spatial diversity (MIMO, relays): creates "secrecy degrees of freedom"

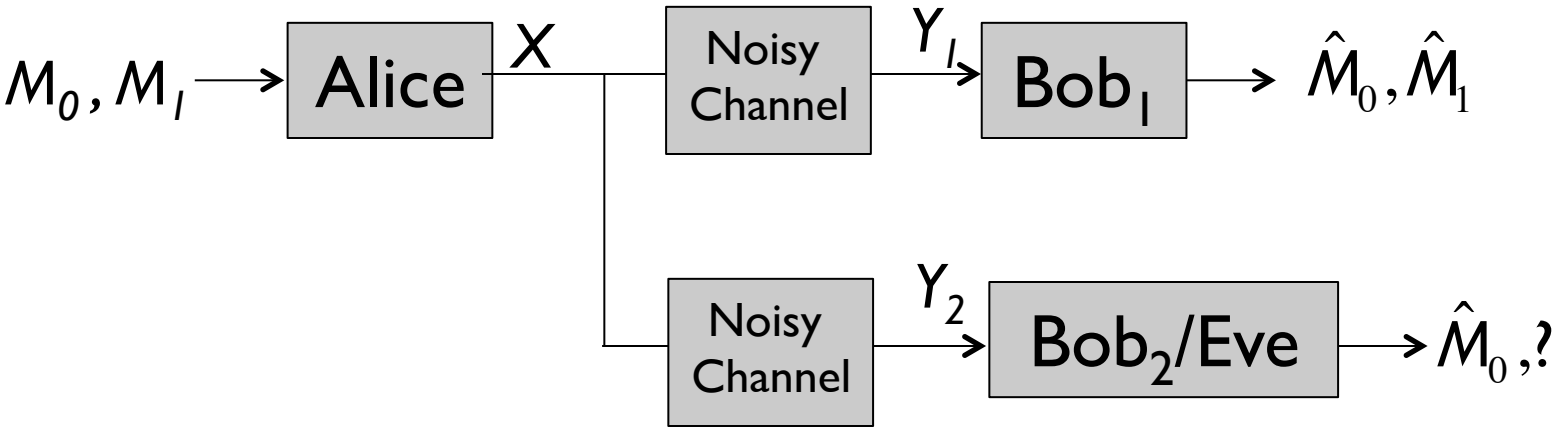
Physical Layer Security in Wireless Networks

- There has been a resurgence of interest in Wyner's ideas, as encryption is impractical for emerging wireless networking paradigms.

- The physical properties of radio propagation (diffusion & superposition) provide opportunities for this, via
  - fading: provides natural degradedness over time
  - interference: allows active countermeasures to eavesdropping
  - spatial diversity (MIMO, relays): creates "secrecy degrees of freedom"

- These phenomena lead to rich secrecy capacity regions for the fundamental channel models used to understand wireless networks.

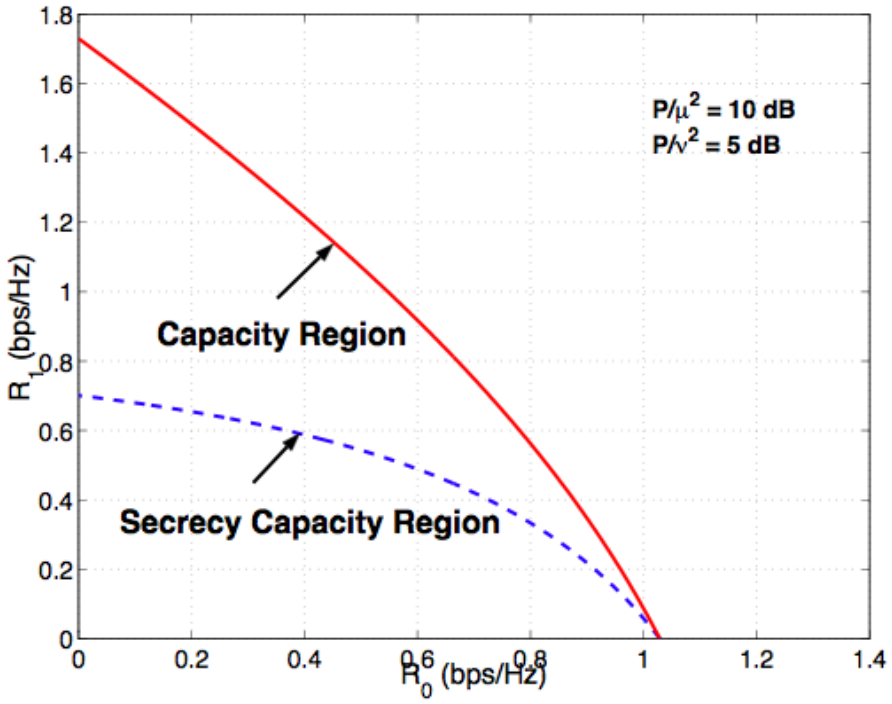
Paradigm: Broadcast Channel with Confidential Messages (BCC)

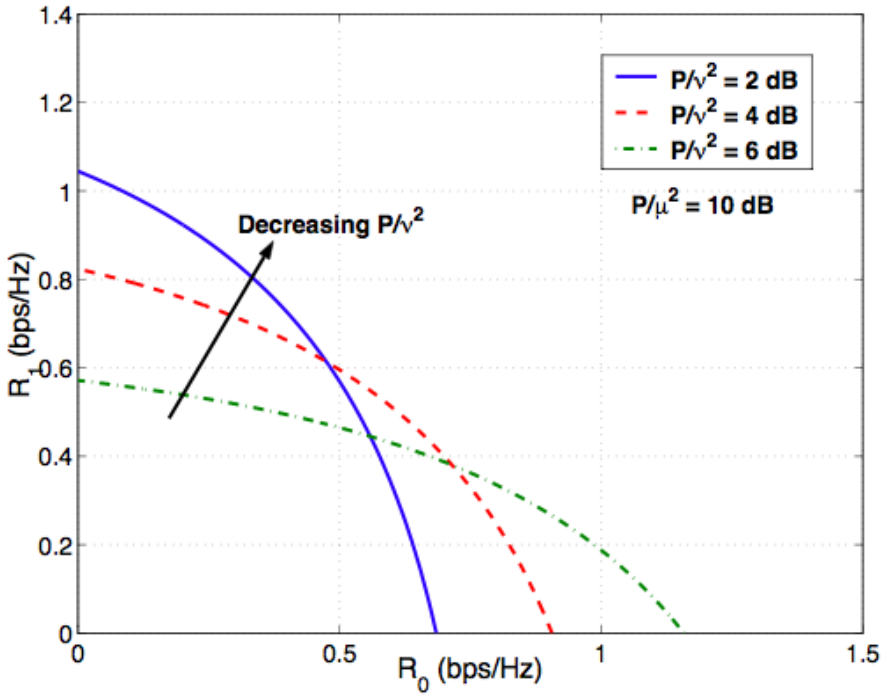


Models content distribution with multicast and unicast content

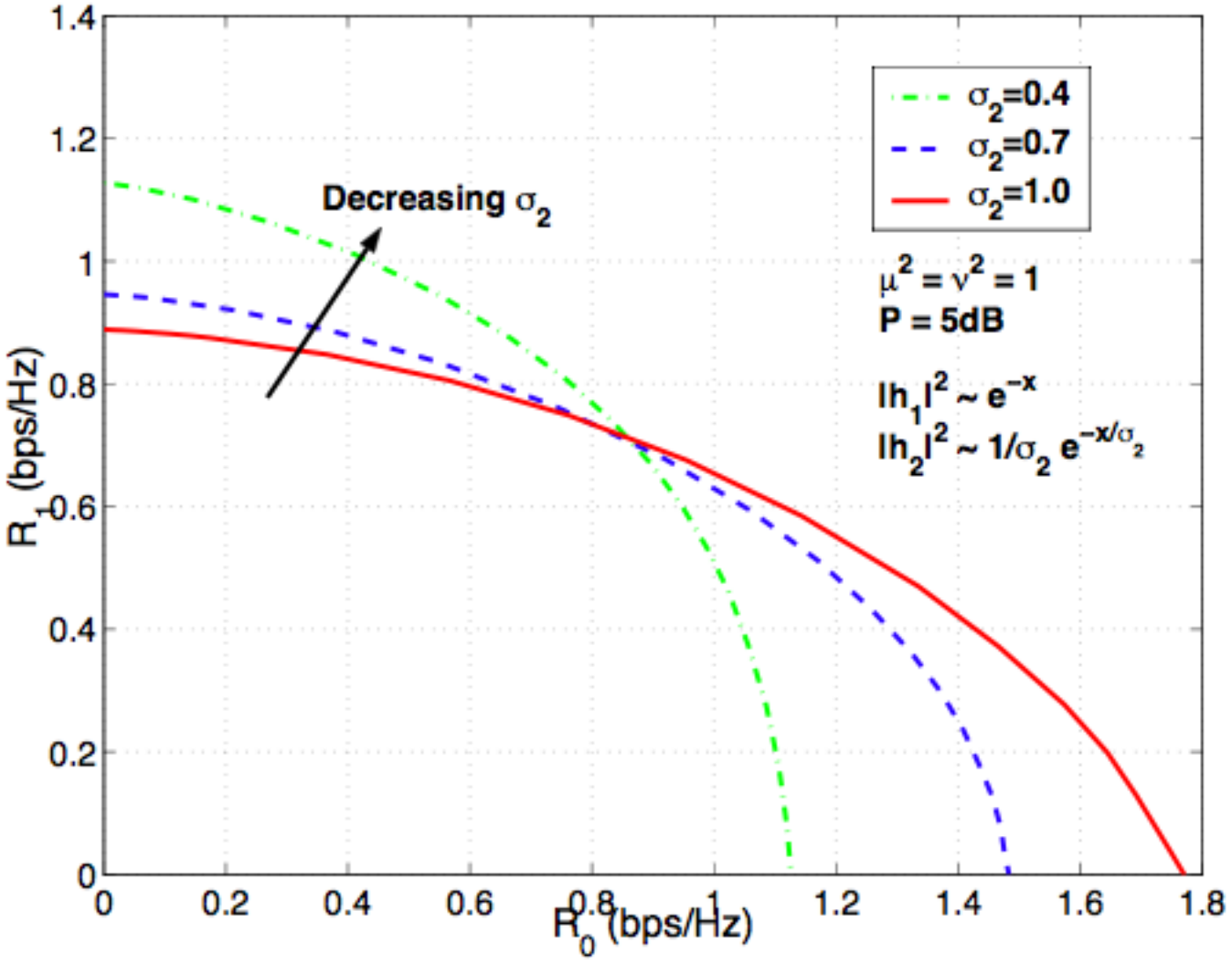
- Csiszár & Körner [1978]: Discrete Memoryless BCC
- Liang, Poor & Shamai [2008]: Gaussian & Fading BCCs

Gaussian BCC: Secrecy Capacity Regions

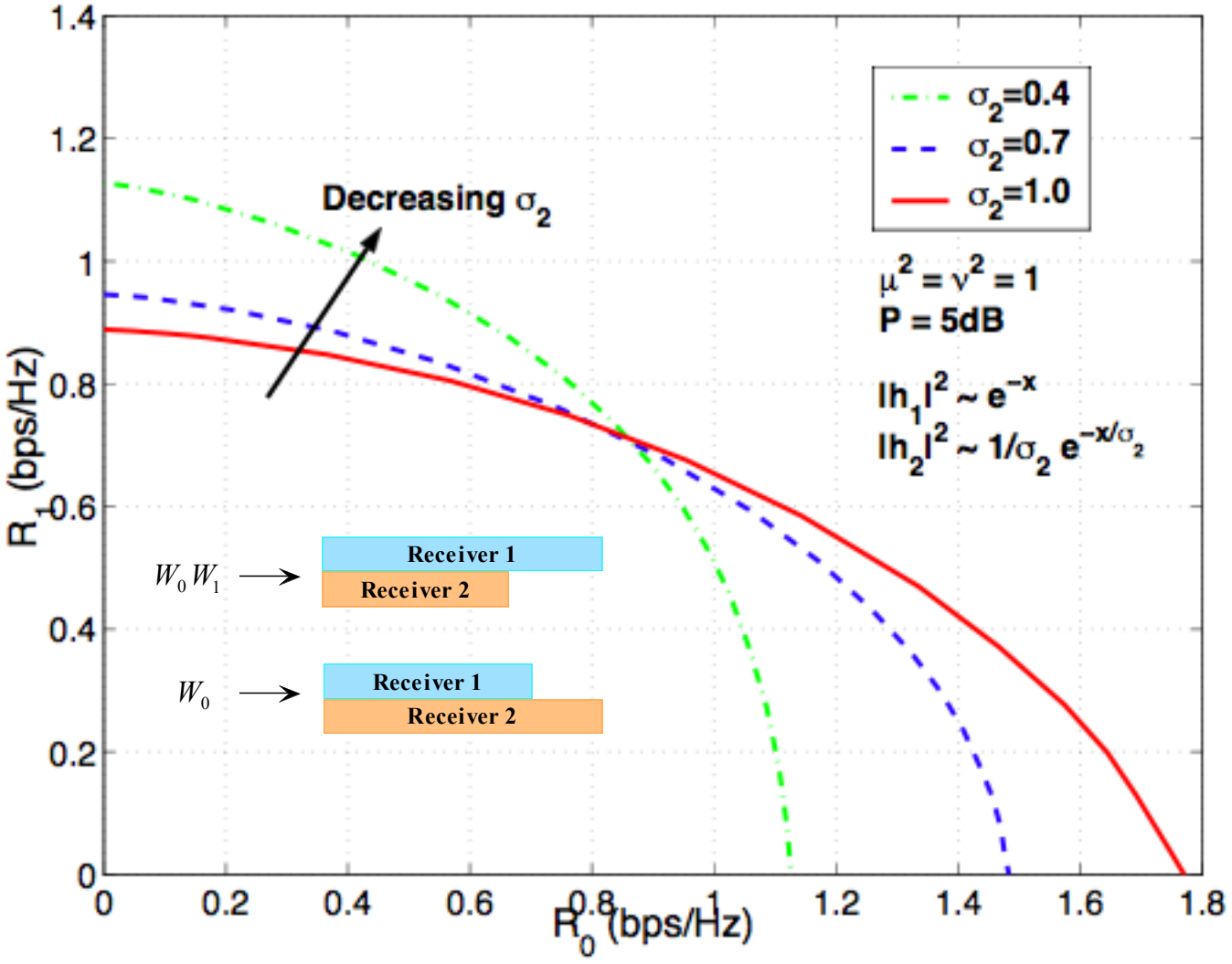




Fading BCC: Secrecy Capacity Region

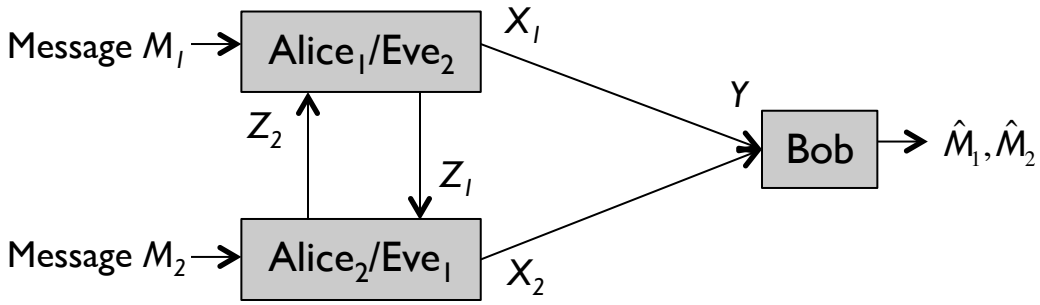


Fading BCC: Secrecy Capacity Region

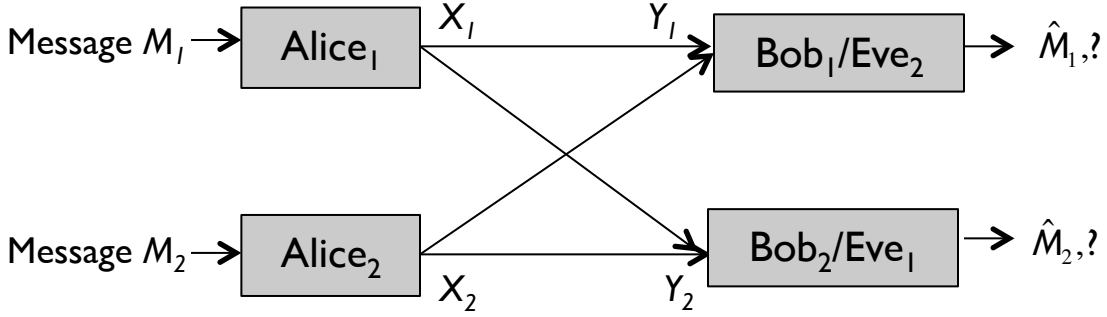


Secrecy in Fundamental Channel Models

- Multiple-Access Channel:

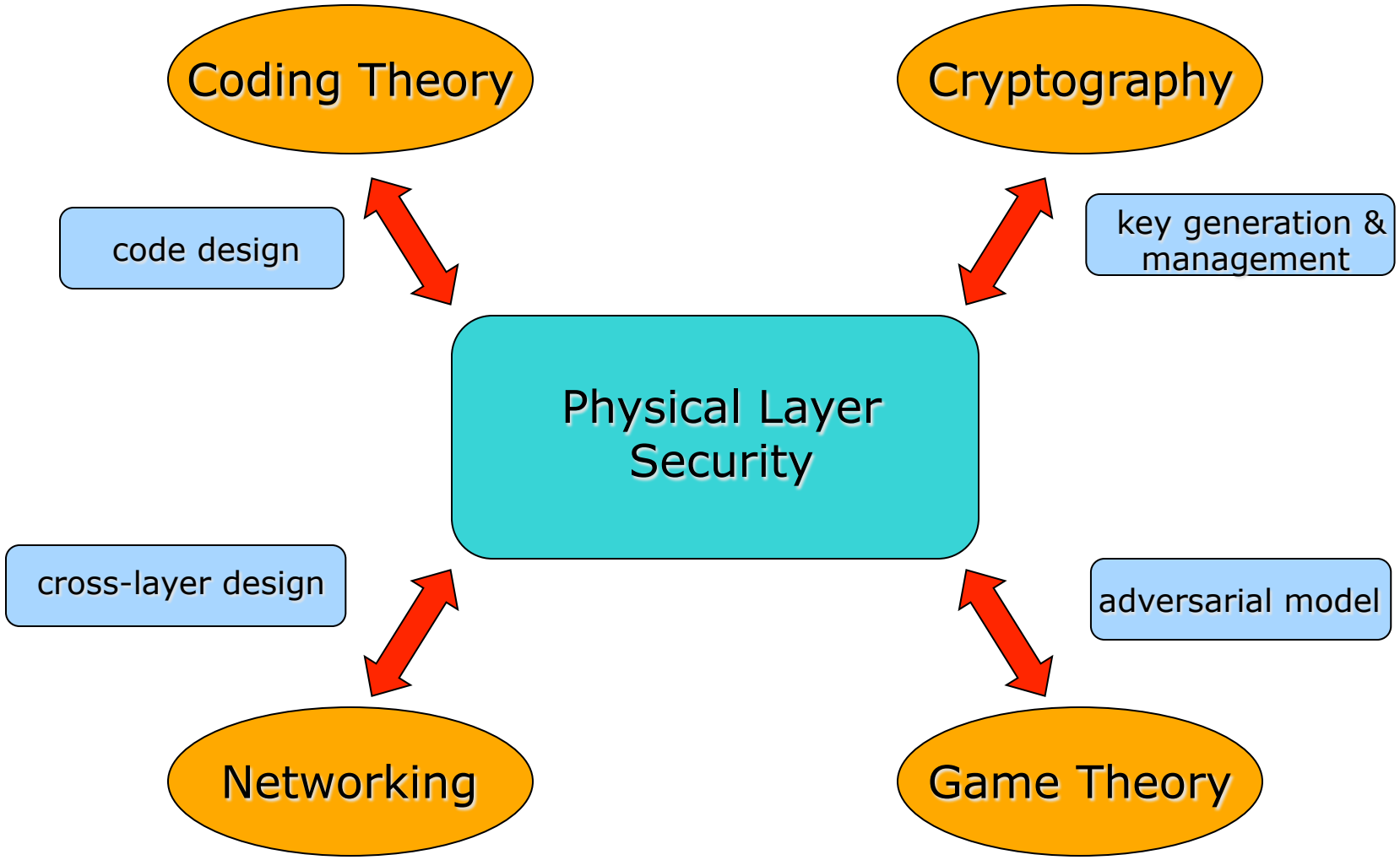


- Interference Channel:



- Relay Channel: Relay cooperates to improve security; or relay is untrusted.
- MIMO Channel: Allows simultaneous secure transmission without rate penalty.

A Rich Area


Coding Theory
Cryptography
code design
key generation & management
Physical Layer Security
cross-layer design
adversarial model
Networking
Game Theory

Privacy-Utility Tradeoffs

with

Applications in Smart Grid

Motivation: Privacy & Utility of Data

- There are many electronic information sources of information about us.
  - Google, Facebook, smart metering, biometric systems, etc.

Motivation: Privacy & Utility of Data

- There are many electronic information sources of information about us.
  - Google, Facebook, smart metering, biometric systems, etc.

- The utility of these sources depends on their accessibility.

Motivation: Privacy & Utility of Data

- There are many electronic information sources of information about us.
  - Google, Facebook, smart metering, biometric systems, etc.

- The utility of these sources depends on their accessibility.
- But, they can also leak private information.

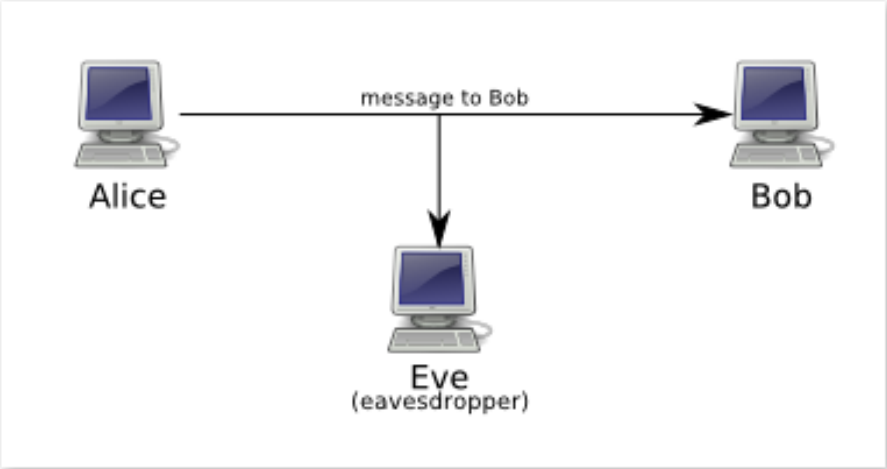
Motivation: Privacy & Utility of Data

- There are many electronic information sources of information about us.
  - Google, Facebook, smart metering, biometric systems, etc.

- The utility of these sources depends on their accessibility.
- But, they can also leak private information.
- How can we characterize this fundamental tradeoff?

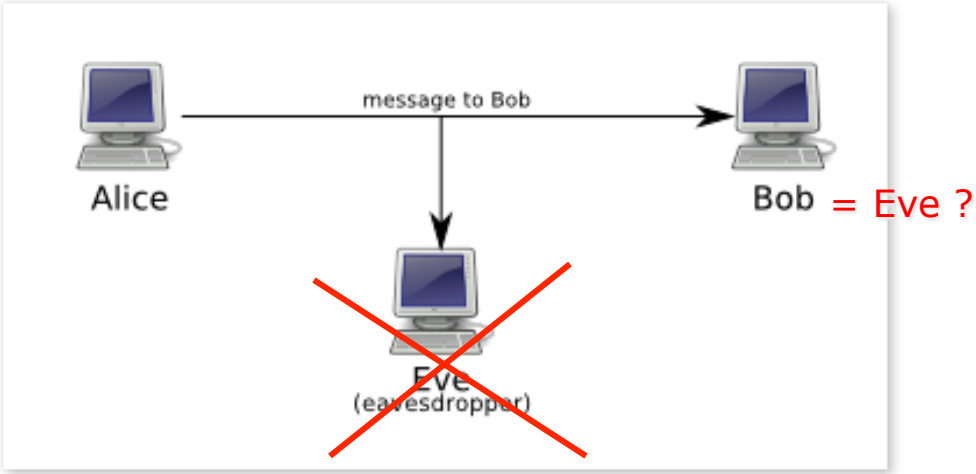
Privacy vs. Secrecy

- Privacy is not secrecy:



Privacy vs. Secrecy

- Privacy is not secrecy:



- Denial of access (secrecy) makes a data source useless.

Privacy-Utility Tradeoff

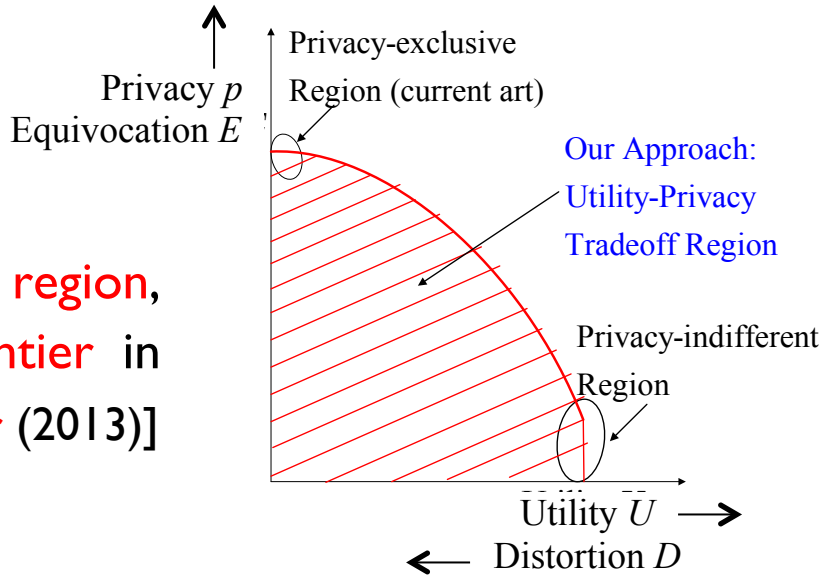
- Data consists of public (revealed) and private (hidden) variables, which are often correlated.

Privacy-Utility Tradeoff

- Data consists of public (revealed) and private (hidden) variables, which are often correlated.
- To characterize the tradeoff between utility and privacy we can
  - measure utility by distortion of public variables as revealed to a user;
  - measure privacy by equivocation of the private variables as revealed.

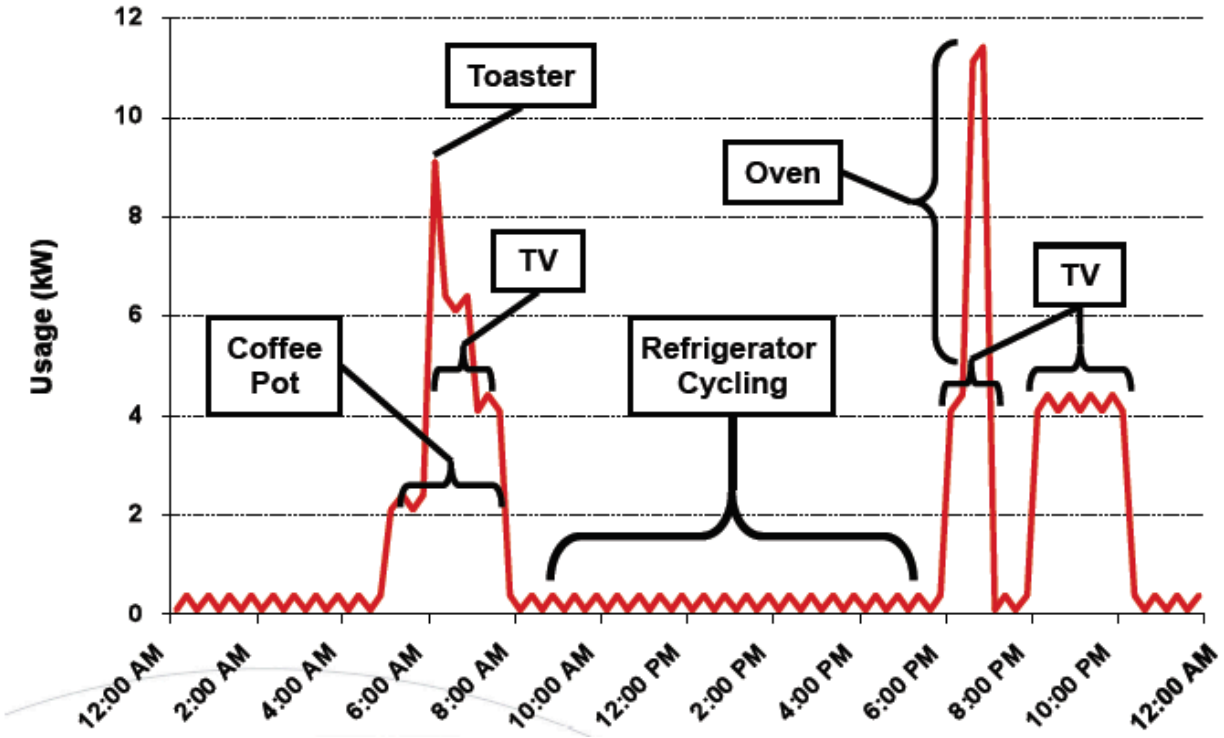
Privacy-Utility Tradeoff

- Data consists of public (revealed) and private (hidden) variables, which are often correlated.
- To characterize the tradeoff between utility and privacy we can
  - measure utility by distortion of public variables as revealed to a user;
  - measure privacy by equivocation of the private variables as revealed.
- Leads to a distortion-equivocation region, whose boundary is the efficient frontier in the tradeoff. [Sankar, Rajagopolan & Poor (2013)]



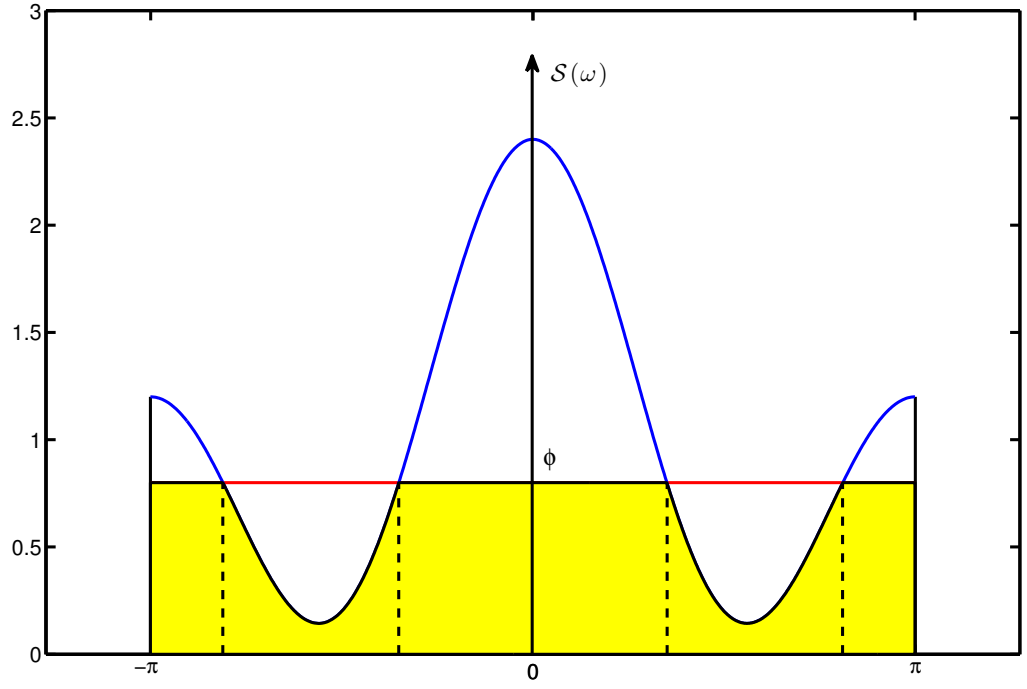
Application: Smart Meter Privacy

- Smart meter data is useful for price-aware usage, load balancing
- But, it leaks information about in-home activity



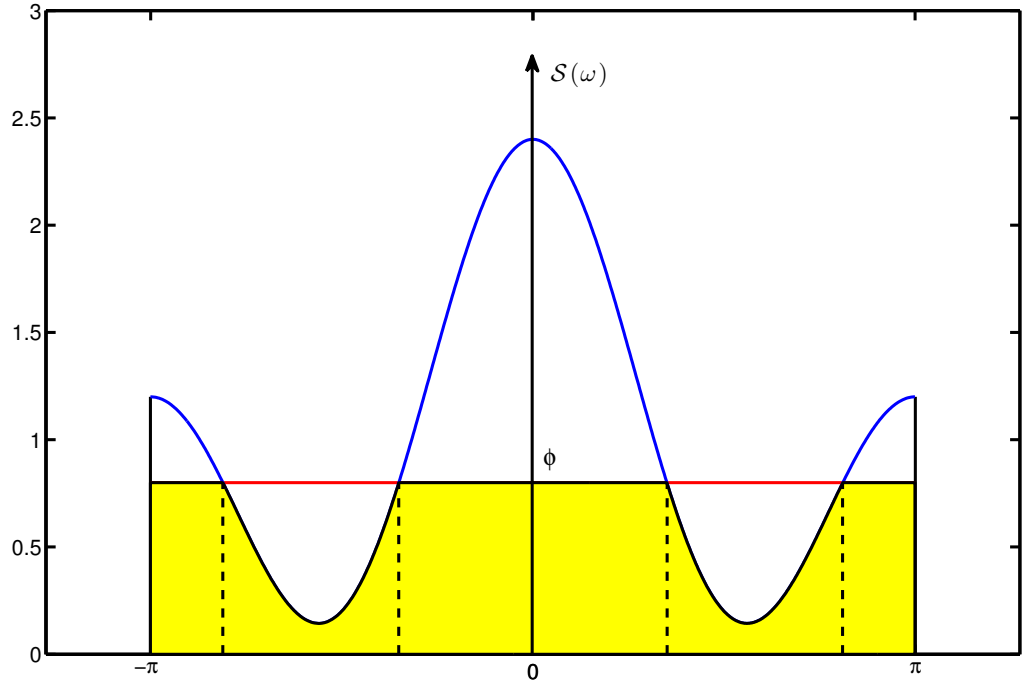
Source Coding Solution

P-U tradeoff leads to a spectral 'reverse water-filling' solution



Source Coding Solution

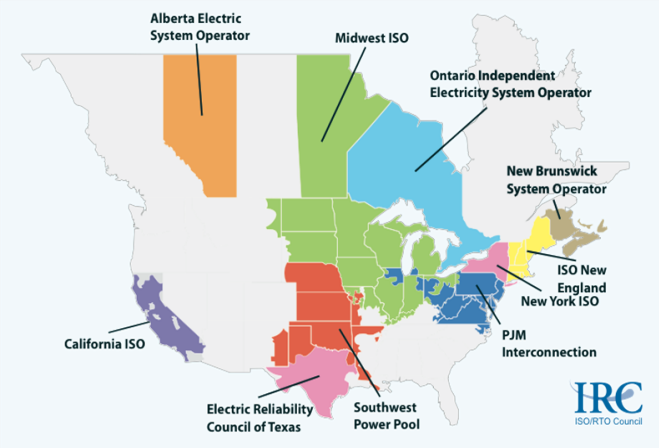
P-U tradeoff leads to a spectral 'reverse water-filling' solution

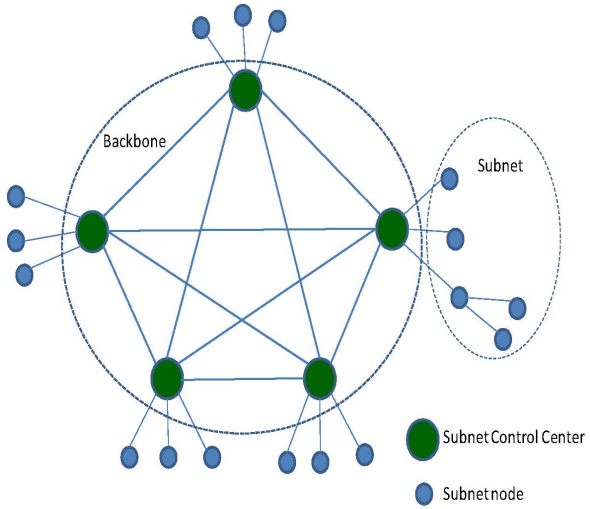


Can also use energy storage to aid privacy – results in a control-theoretic solution [Tan-Gunduz-Poor, 2013] [Yang-Chen-Zhang-Poor, 2015]

Competitive Privacy: Motivating Example

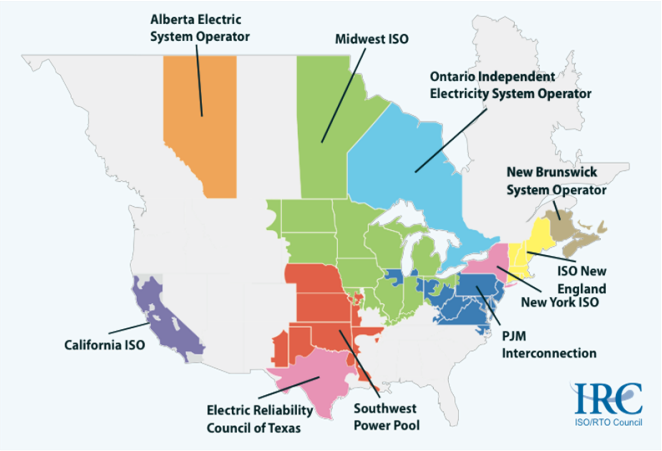
- N.A. Grid: interconnected regional transmission organizations (RTOs) which
  - need to share state measurements for reliability of state estimation (utility)
  - wish to withhold information for economic competitiveness (privacy)

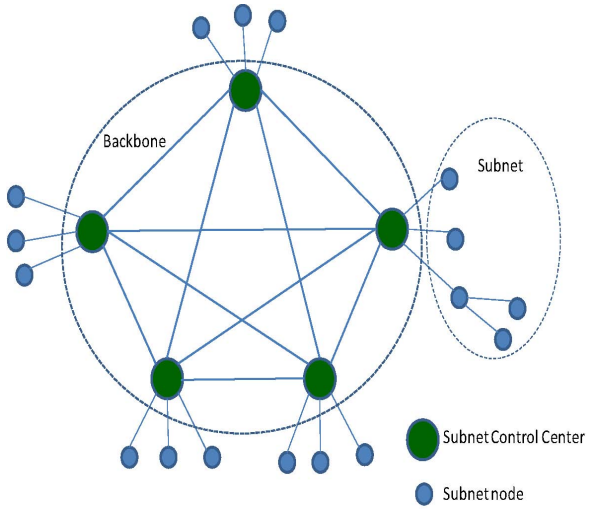




Competitive Privacy: Motivating Example

- N.A. Grid: interconnected regional transmission organizations (RTOs) which
  - need to share state measurements for reliability of state estimation (utility)
  - wish to withhold information for economic competitiveness (privacy)

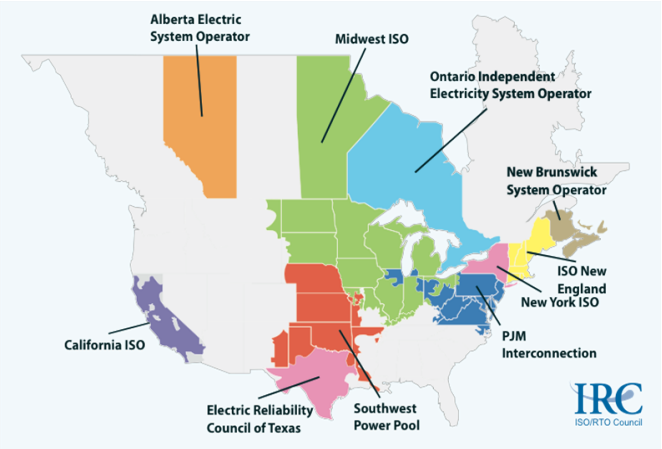


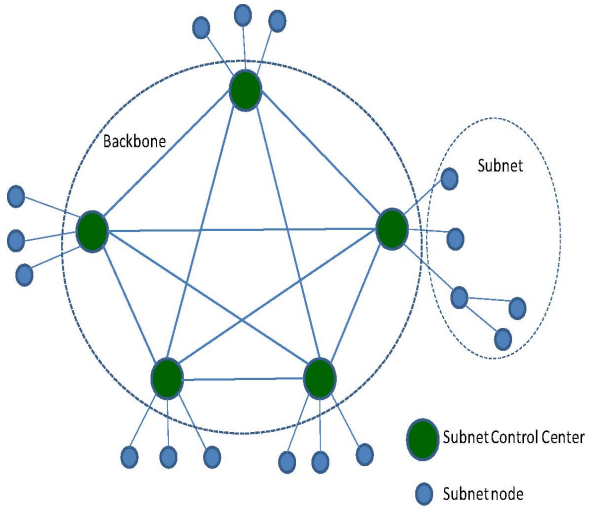


- Leads to a problem of competitive privacy.

Competitive Privacy: Motivating Example

- N.A. Grid: interconnected regional transmission organizations (RTOs) which
  - need to share state measurements for reliability of state estimation (utility)
  - wish to withhold information for economic competitiveness (privacy)

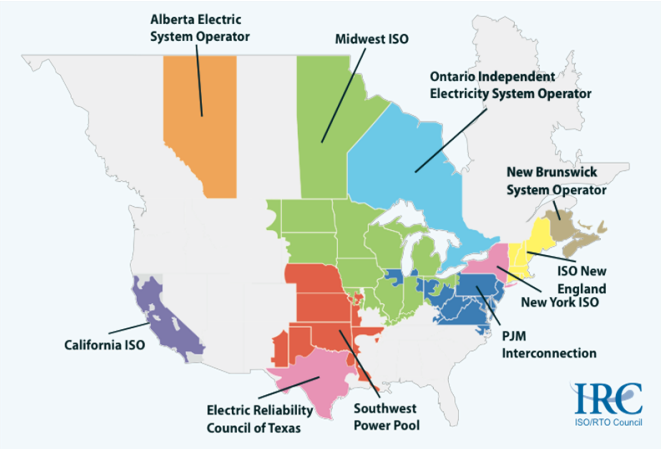


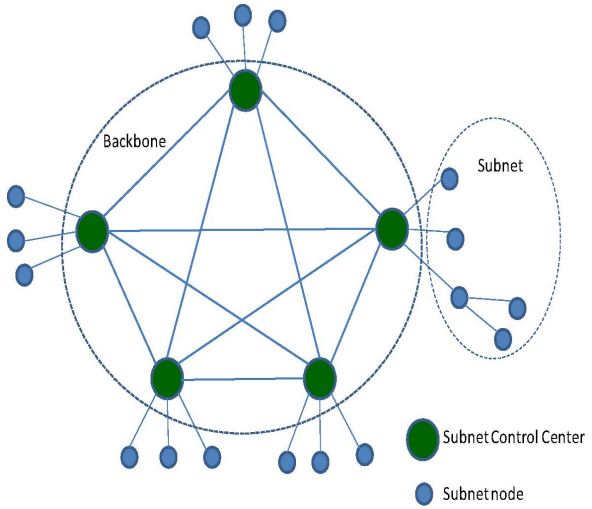


- Leads to a problem of competitive privacy.
- Optimal source coding (Wyner-Ziv) yields optimal information exchange.

Competitive Privacy: Motivating Example

- N.A. Grid: interconnected regional transmission organizations (RTOs) which
  - need to share state measurements for reliability of state estimation (utility)
  - wish to withhold information for economic competitiveness (privacy)

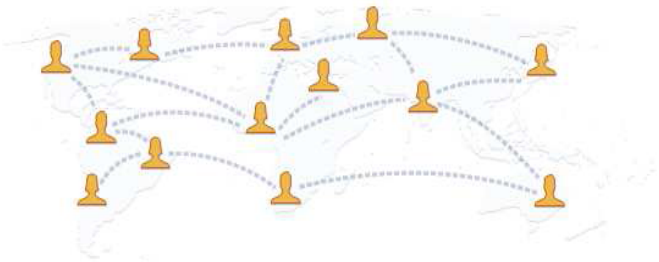




- Leads to a problem of competitive privacy.
- Optimal source coding (Wyner-Ziv) yields optimal information exchange.
- Competition invokes game theory.

Other Potential Applications

Biometric Systems: tradeoff between security & privacy



Social Networks: tradeoff between sharing & privacy

E-Commerce: tradeoff between profit & privacy

Summary

- Information theory can help understand the fundamental ability of the radio channel to provide confidentiality of wireless data.

Summary

- Information theory can help understand the fundamental ability of the radio channel to provide confidentiality of wireless data.

- A fundamental tradeoff between privacy and utility of data sources can also be viewed in an information theoretic setting.

Summary

- Information theory can help understand the fundamental ability of the radio channel to provide confidentiality of wireless data.

- A fundamental tradeoff between privacy and utility of data sources can also be viewed in an information theoretic setting.

- Examples from smart grid: smart metering and competitive privacy give rise to tradeoffs between fidelity and information leakage.

Summary

- Information theory can help understand the fundamental ability of the radio channel to provide confidentiality of wireless data.
- A fundamental tradeoff between privacy and utility of data sources can also be viewed in an information theoretic setting.
- Examples from smart grid: smart metering and competitive privacy give rise to tradeoffs between fidelity and information leakage.
- These are theoretical constructs, but they point to potential practical solutions.


Thank You!