Physical Layer Security in Wireless Networks

An Information Theoretic Perspective

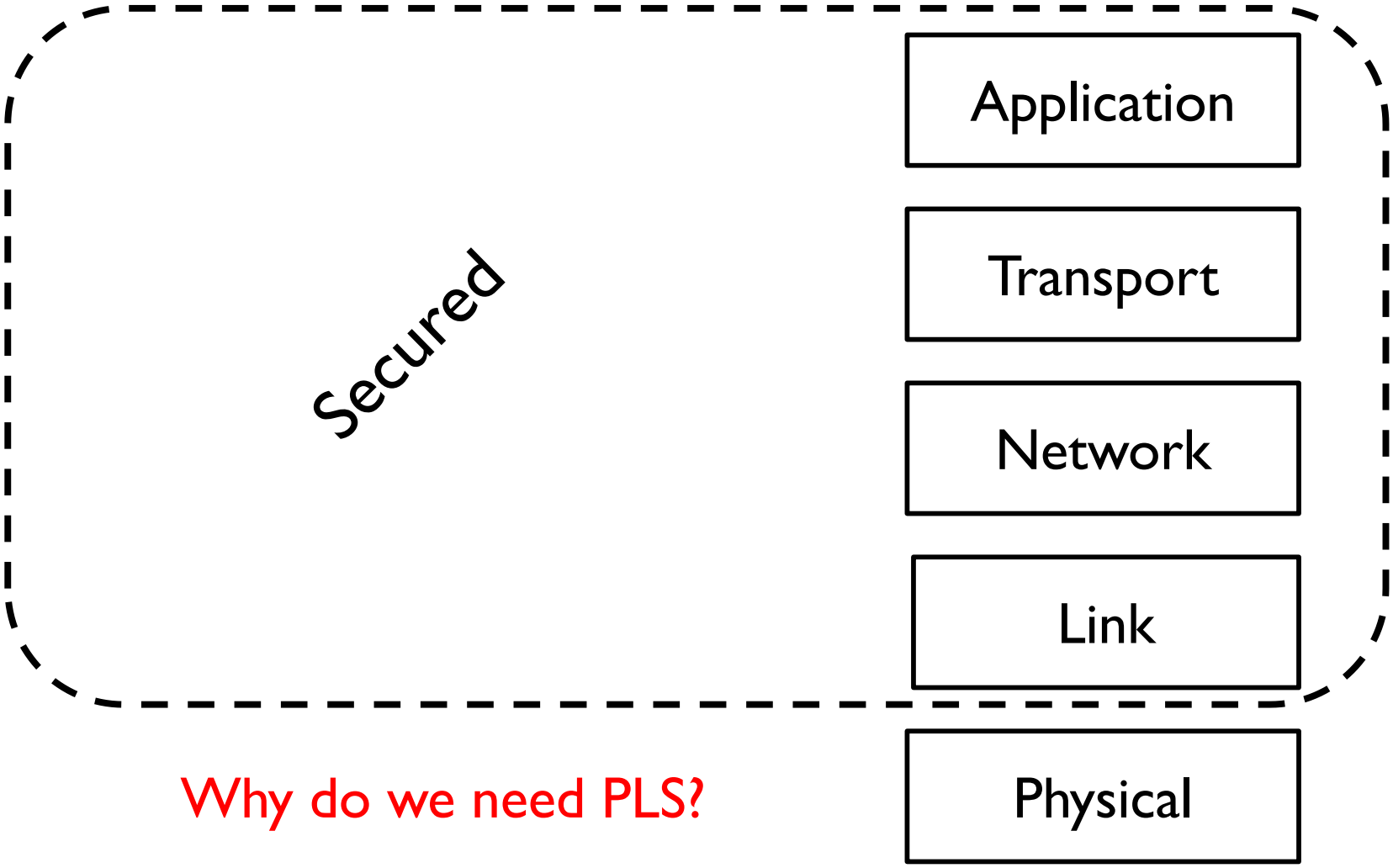
Vince Poor
(poor@princeton.edu)

Thanks to:

Arsenia Chorti (ENSEA), Mahdi Shakiba Herfeh (ENSEA) and Miroslav G. Mitev (Essex)

M. S. Herfeh, A. Chorti & H. V. Poor, "Physical Layer Security: Authentication, Integrity and Confidentiality." In *Physical Layer Security*, Khoa N. Le, Ed. (Springer Nature, 2021), to appear.

Today's Security Architecture



Why do we need PLS?

Standard Crypto Systems

- No known feasible attacks
- Widely employed and tested
- Trustworthy authentication

- Built on unproven assumptions
- PHY connection assumed established
- Computationally intensive
- Require significant infrastructure

Physical Layer Security

- Quantum secure
- On-the-fly secret key generation
- Fast and lightweight implementation

- Assumptions on Eve's channel
- Bounds not categorized on finite blocks
- Testing – still in infancy

A Prime Example: IoT

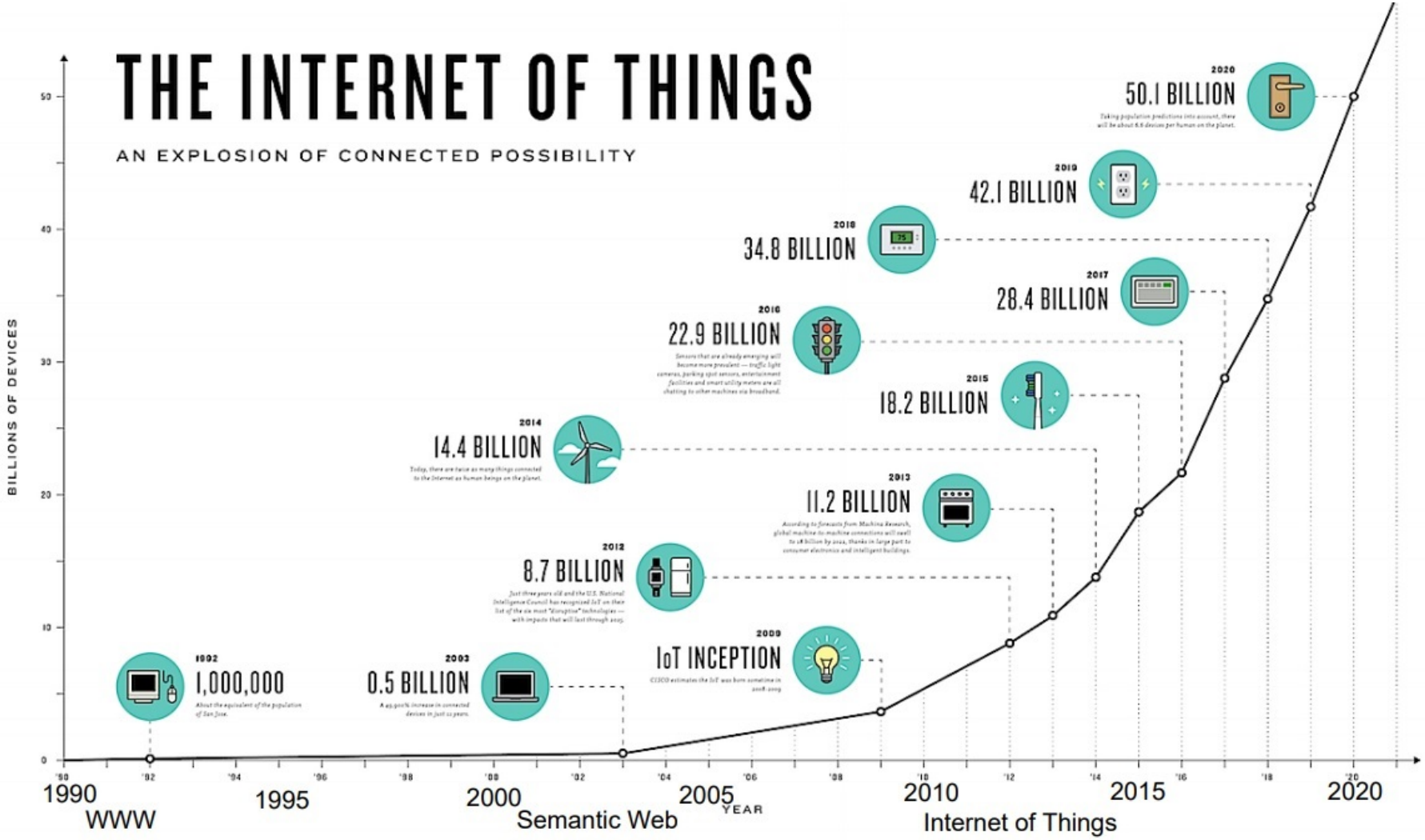


Figure source:
https://www.computer.org/

IoT Security – A Major Concern

- IoT vulnerabilities to cyber attacks → Mostly concern *personal privacy and security*

WIRED

AUGUST 10, 2018 | LOUISE MATSAKIS

Hackable Touchscreens Could Spy on Hotel Rooms and Meetings

The technology company Crestron makes touchscreen panels and other equipment for places like conference rooms, which a researcher found can be turned into hidd...

DECEMBER 20, 2017 | BRIAN BARRETT

Don't Get Your Kid an Internet-Connected Toy

They can be hacked. They're a privacy nightmare. This year, it's not too late to keep the IoT toys away from the tree.

MARCH 2, 2017 | LILY HAY NEWMAN

Medical Devices Are the Next Security Nightmare

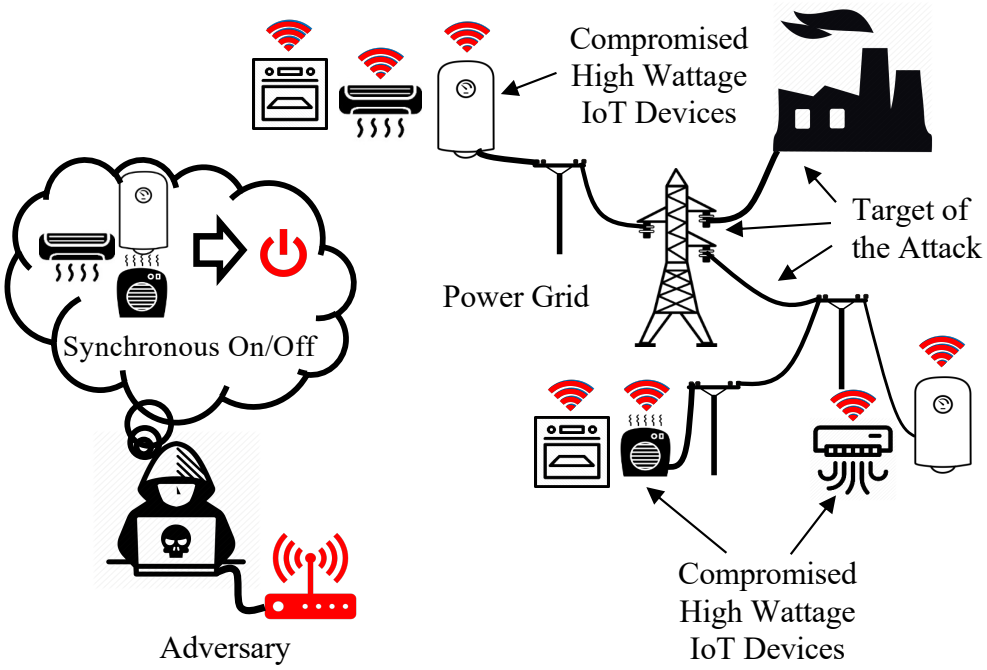
More internet-connected medical devices flood into healthcare industry every day, but we're not moving fast enough to defend them.

An Example of What Can Go Wrong

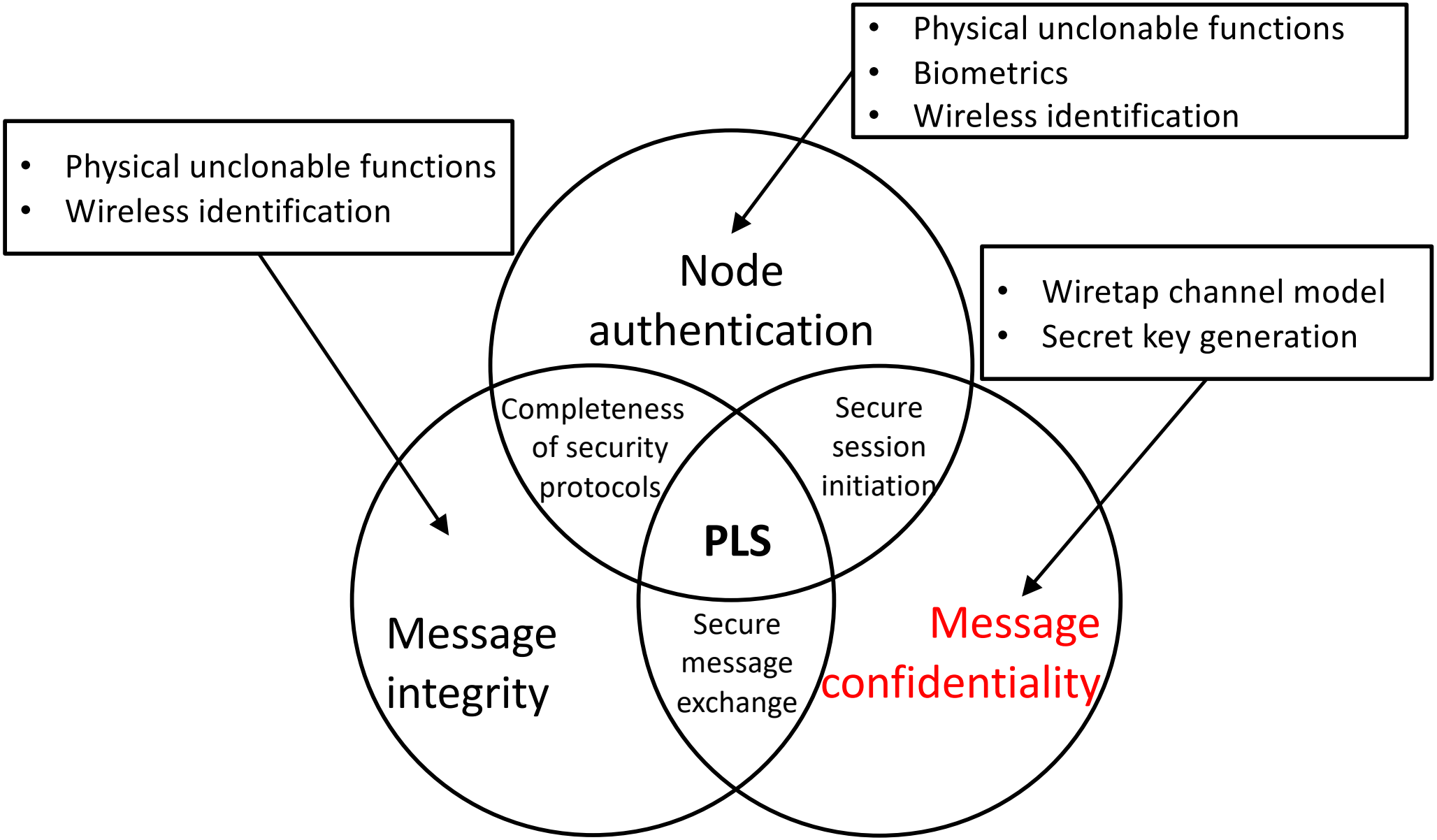
[Soltan, Mittal, Poor, USENIX'18]

- Manipulation of demand via IoT: Botnets controlling high-wattage IoT devices (air conditioners, refrigerators, etc.) can disrupt the power grid.

- A Mirai-sized (600,000 bots) botnet of water heaters can change the demand instantly by 3GW – similar to having access to the largest currently deployed nuclear plant!



PLS Can Offer



Overview of Today's Talk

The theme:

- A role for information theory in this area

Focus mainly on message confidentiality and privacy:

- Message confidentiality in data transmission systems
- Privacy in sensing systems

Other issues – some newer some older (briefly):

- Authentication, security in MANETs, attacks on sensor networks

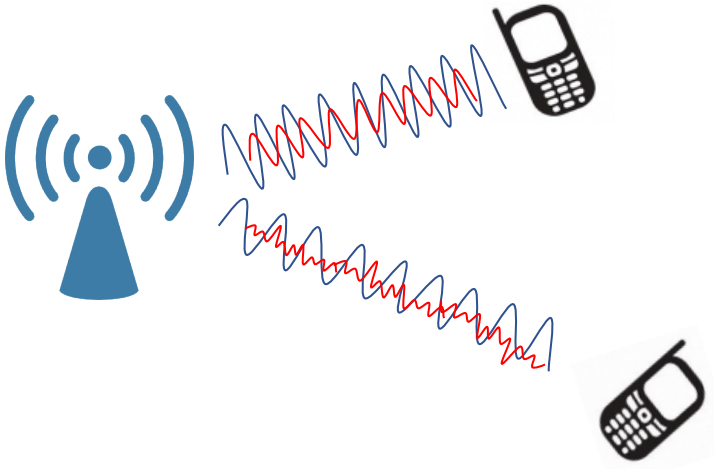
Message Confidentiality

in

Transmission Systems

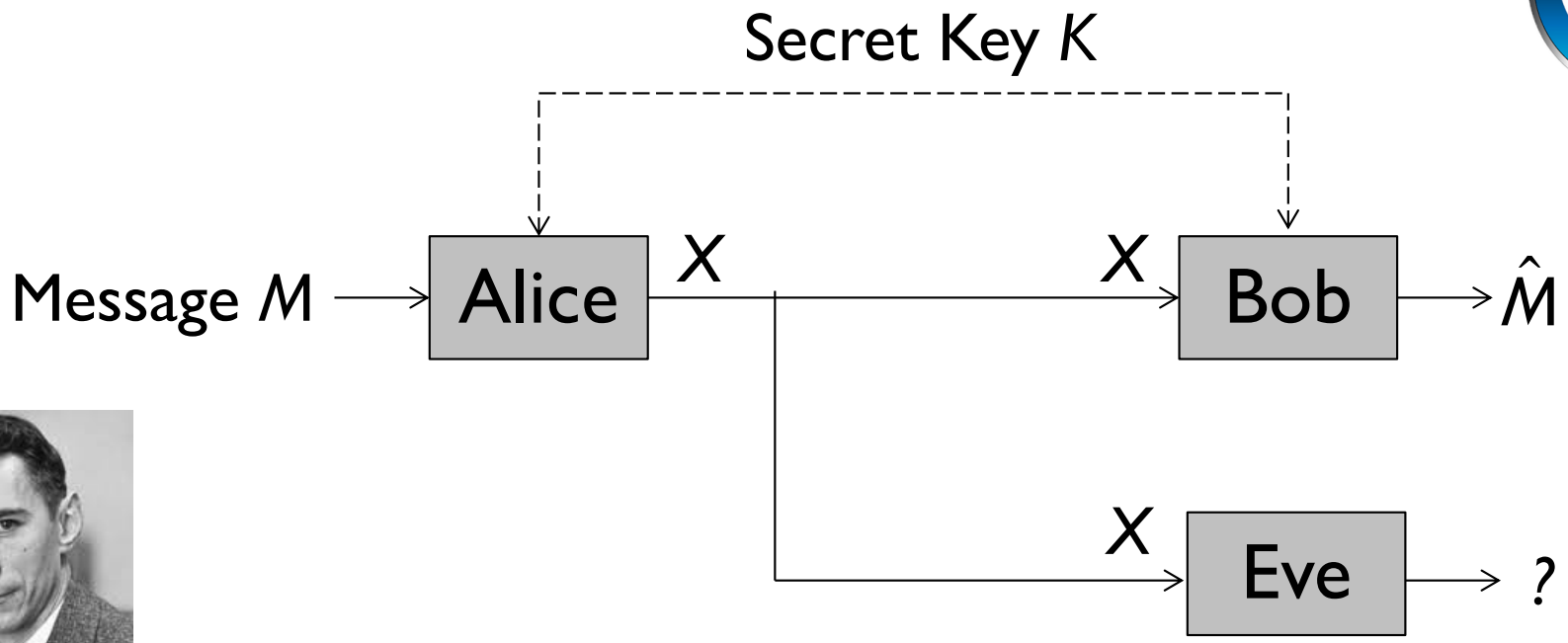
Rethinking Security Design

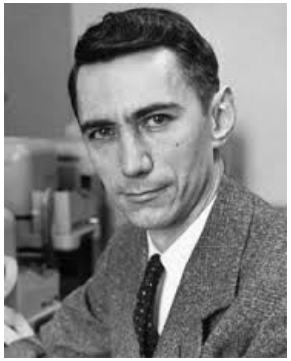
- Conventionally a higher layer issue: encryption, key distributions, …
- Difficult with massive number of devices (esp. with no infrastructure), low cost, low latency.



- Physical layer security provides security by exploiting imperfections in physical channels: noise, fading, …
- Joint encoding for reliability and security.

Information Theoretic Security:
Shannon's Model



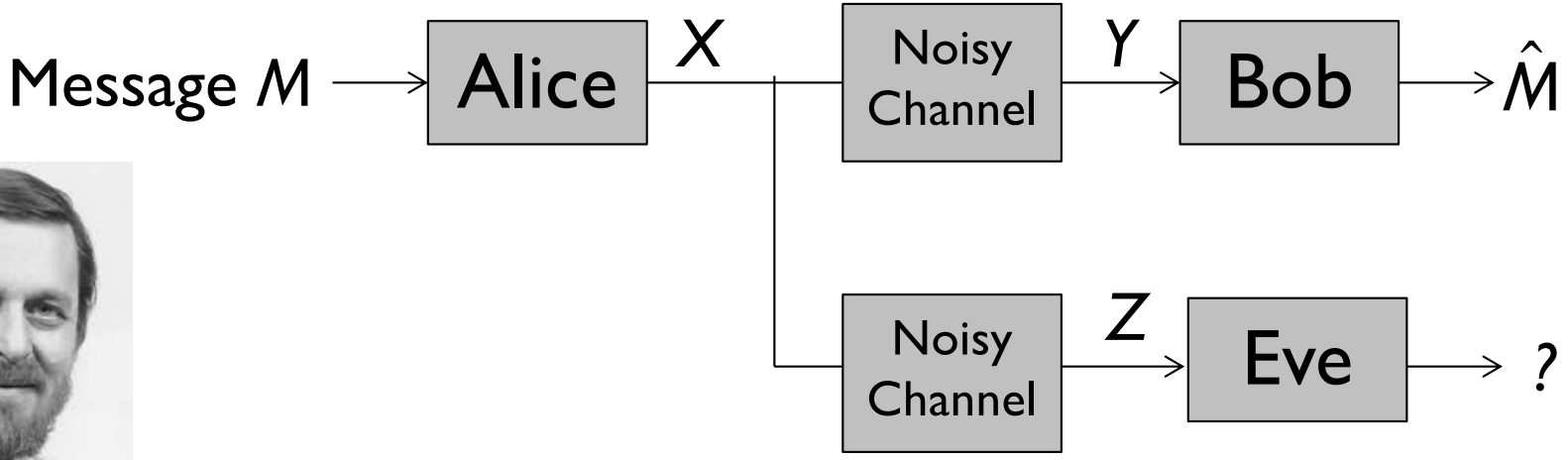


Shannon (1949): For cipher, perfect secrecy requires a one-time pad.

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

Information Theoretic Security:
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

- There has been a resurgence of interest in these ideas.

- In general, the legitimate receiver needs an advantage over the eavesdropper – either a secret shared with the transmitter, or a better channel.

Physical Layer Security

- There has been a resurgence of interest in these ideas.

  - In general, the legitimate receiver needs an advantage over the eavesdropper – either a secret shared with the transmitter, or a better channel.

- 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"
  - random channels: sources of common randomness for key generation

Physical Layer Security

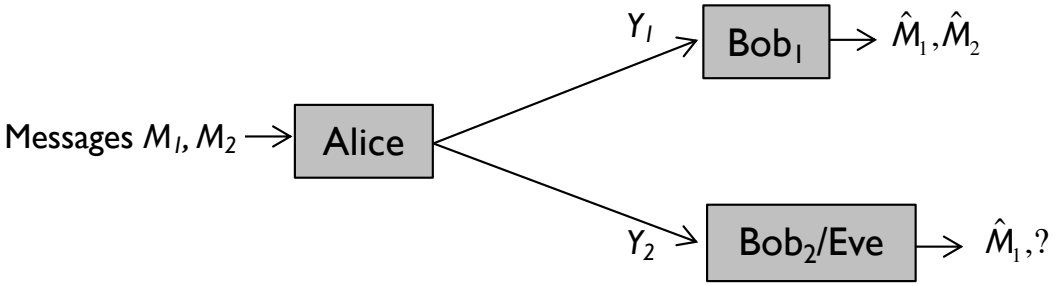
- There has been a resurgence of interest in these ideas.

  - In general, the legitimate receiver needs an advantage over the eavesdropper – either a secret shared with the transmitter, or a better channel.

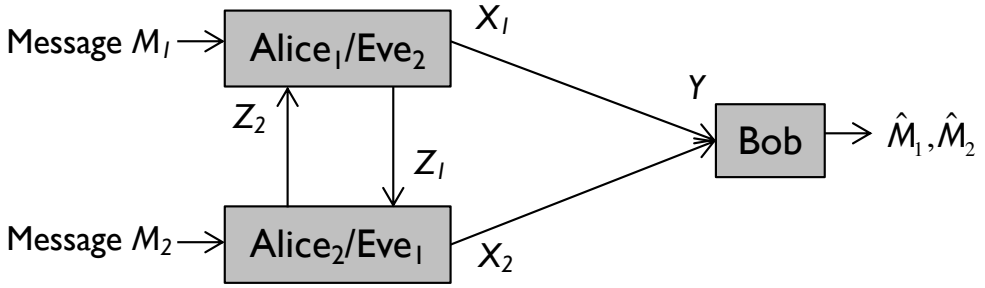
- The physical properties of radio propagation (diffusion & superposition) provide opportunities for this, via
  - fading: provides natural degradedness over time
  - interference: allows active countermeasures to eavesdropping
  - spatial diversity (MIMO, relays): creates "secrecy degrees of freedom"
  - random channels: sources of common randomness for key generation
- The first three of these phenomena lead to rich secrecy capacity regions for the fundamental channel models used to understand wireless networks.

Secrecy in Fundamental Channel Models

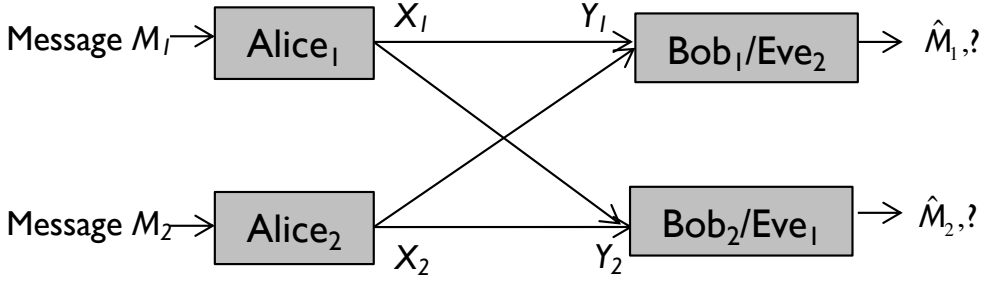
- Broadcast Channels:



- Multiple-Access Channels:



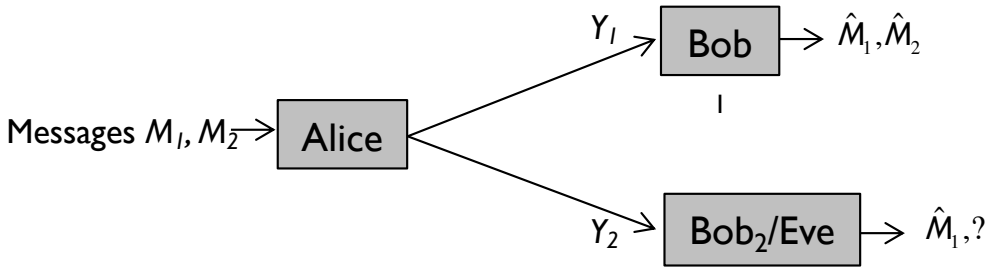
- Interference Channels:

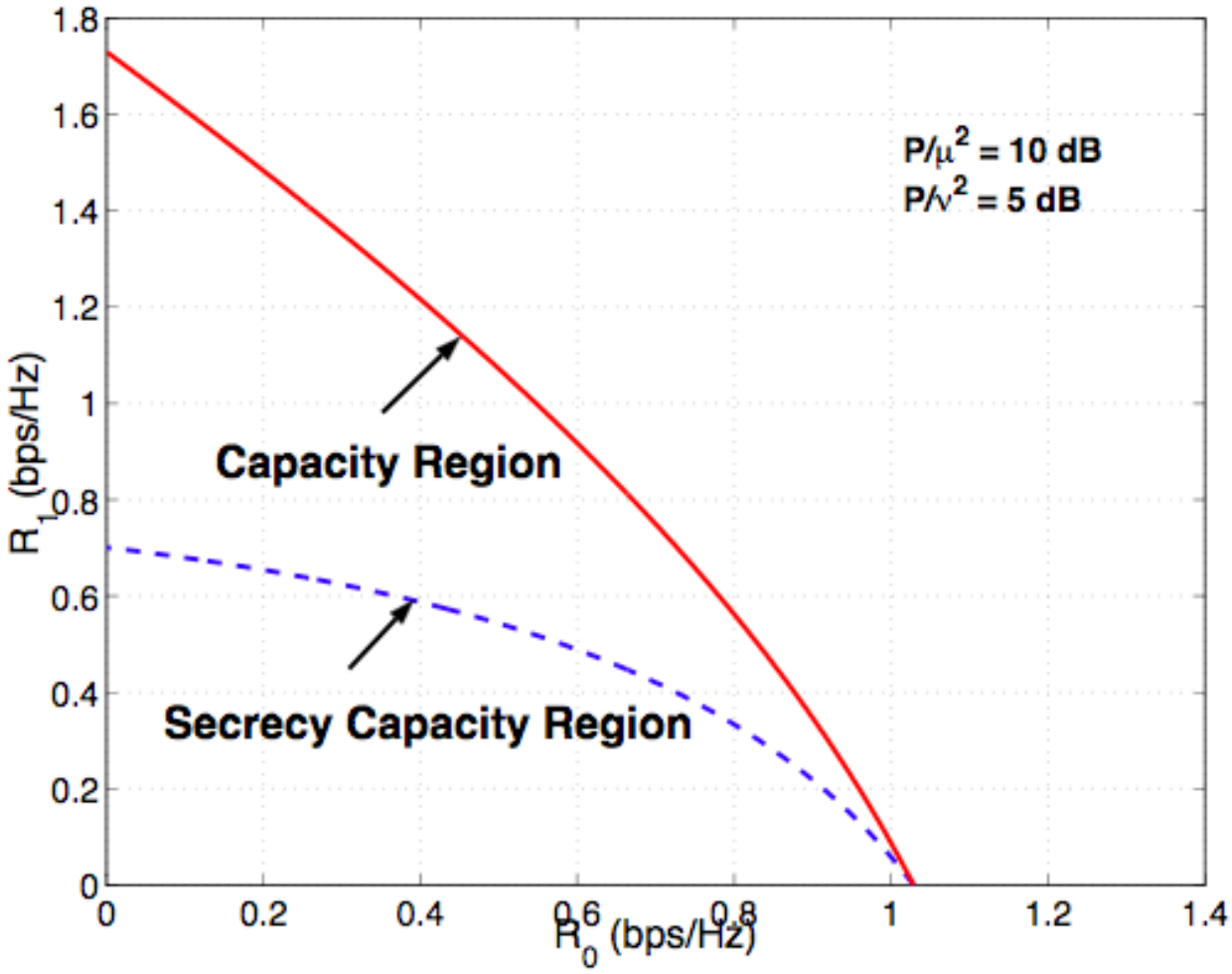


- Relay Channels, MIMO Channels, etc.

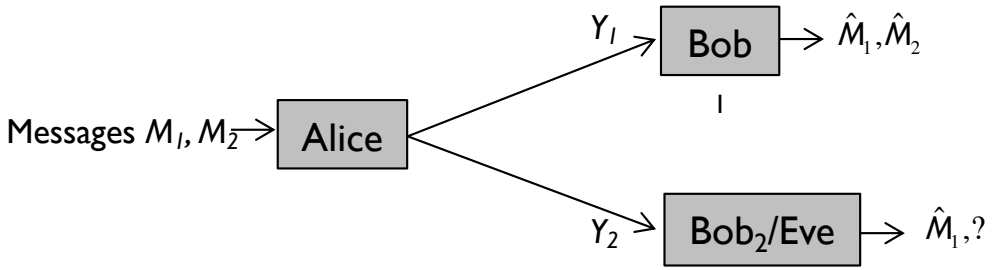
Poor, Schaefer (2017) Wireless Physical Layer Security PNAS

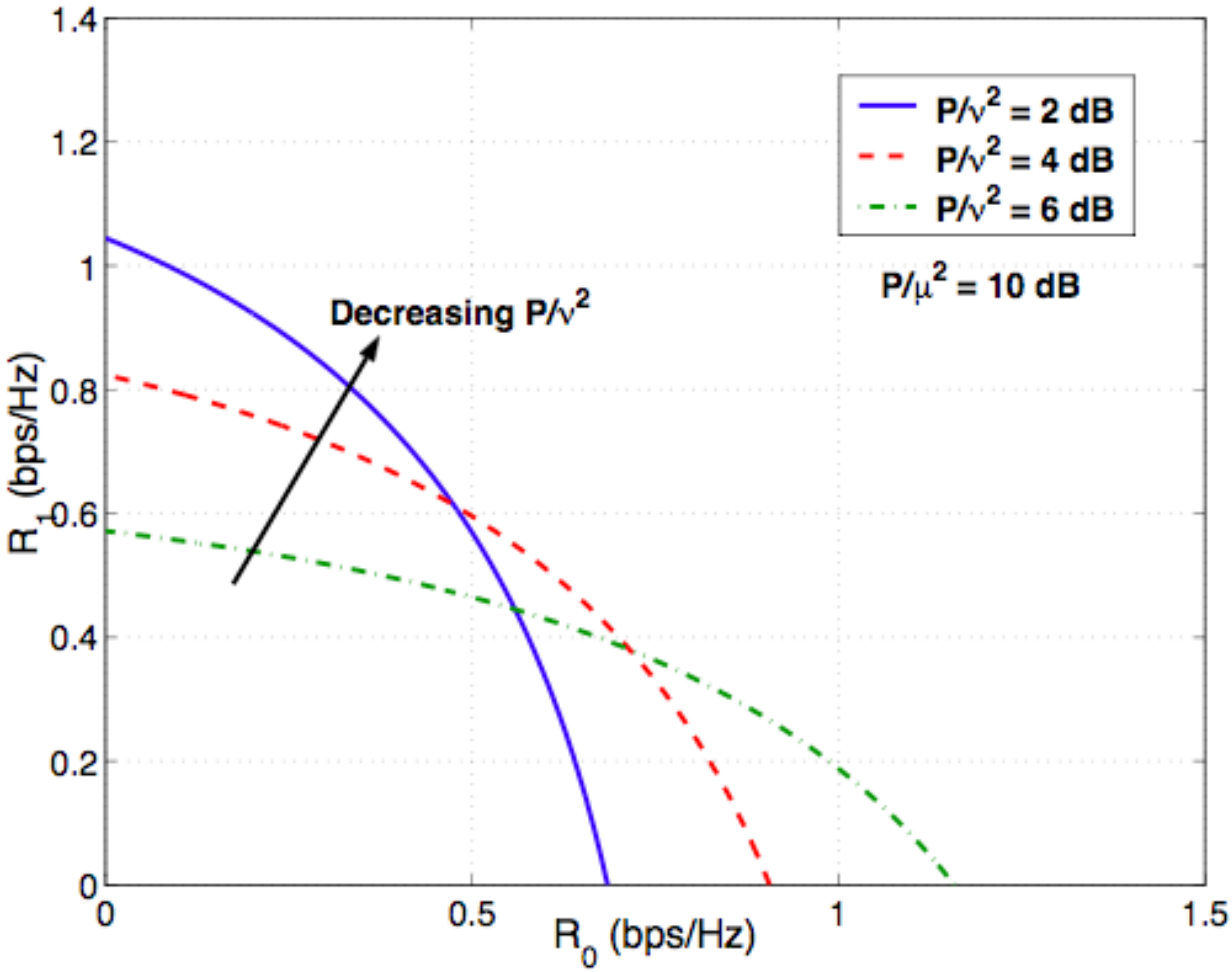
E.g., the Gaussian Broadcast Channel



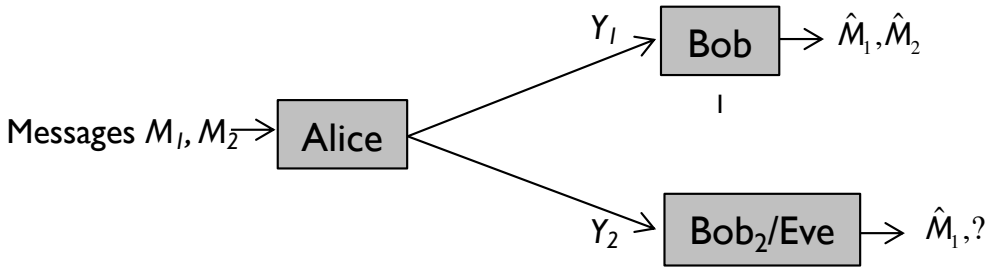


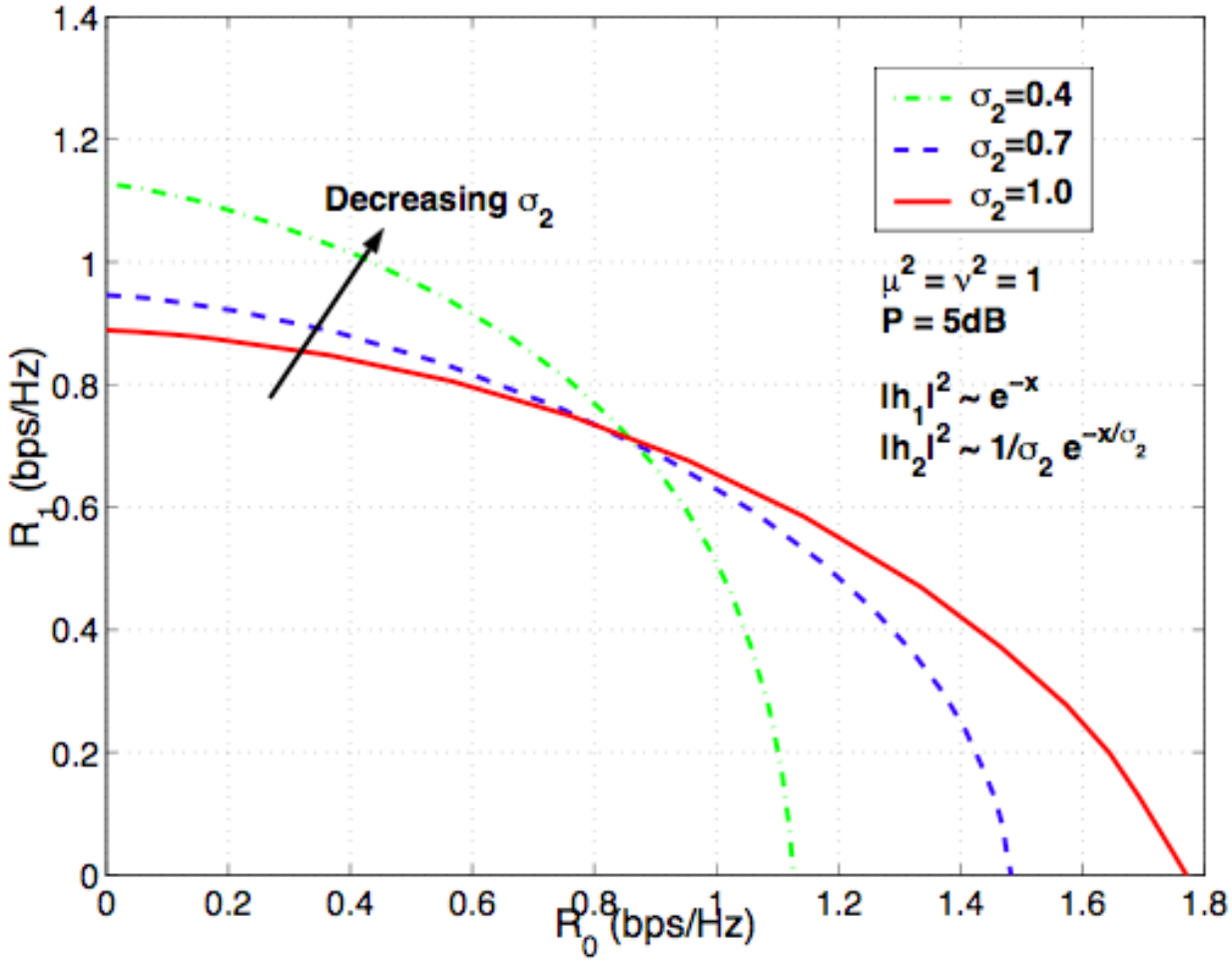
E.g., the Gaussian Broadcast Channel



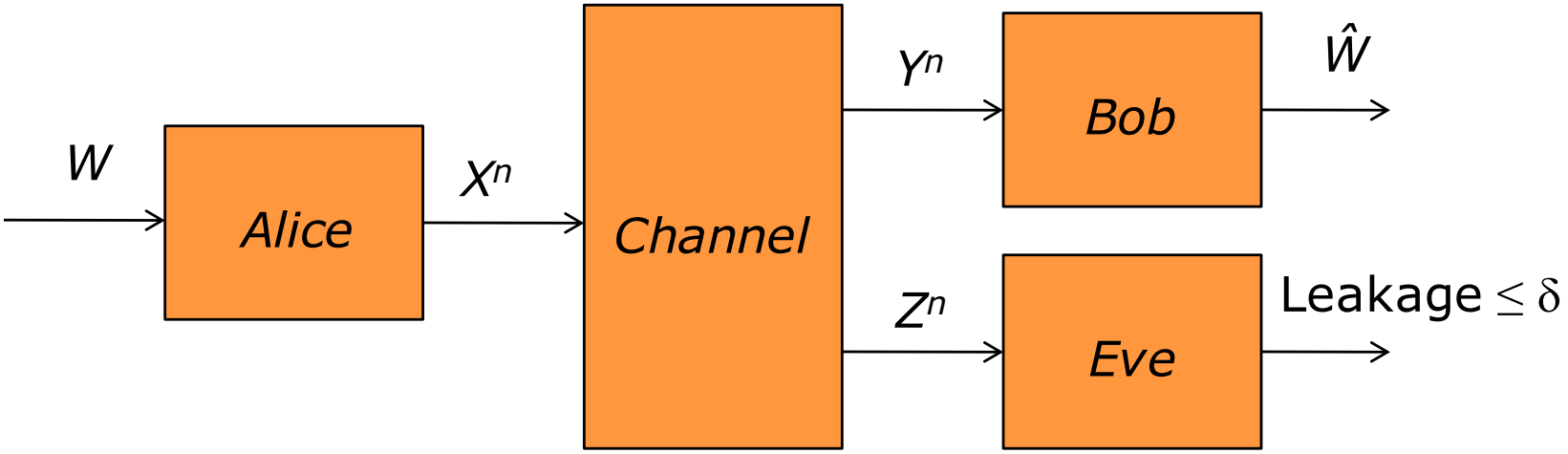


E.g., the Fading Gaussian BC





Wiretap Channel and Secrecy Capacity

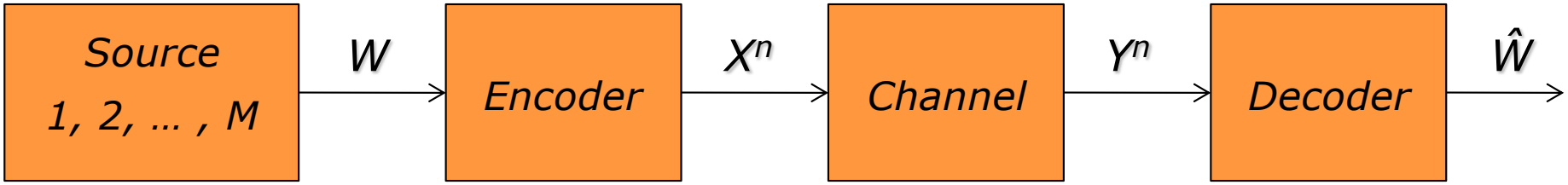


- Secrecy capacity: largest rate in the asymptotic regime of
  - Blocklength $n \to \infty$
  - Probability of error $\mathbb{P}\left(W \neq \hat{W}\right) \to 0$
  - Information leakage $\delta \to 0$

$$C_s = \max_{P_X} \{I(X;Y) - I(X;Z)\}$$

- Limitation: not suitable for low-latency applications as in IoT.

Finite Blocklength Information Theory



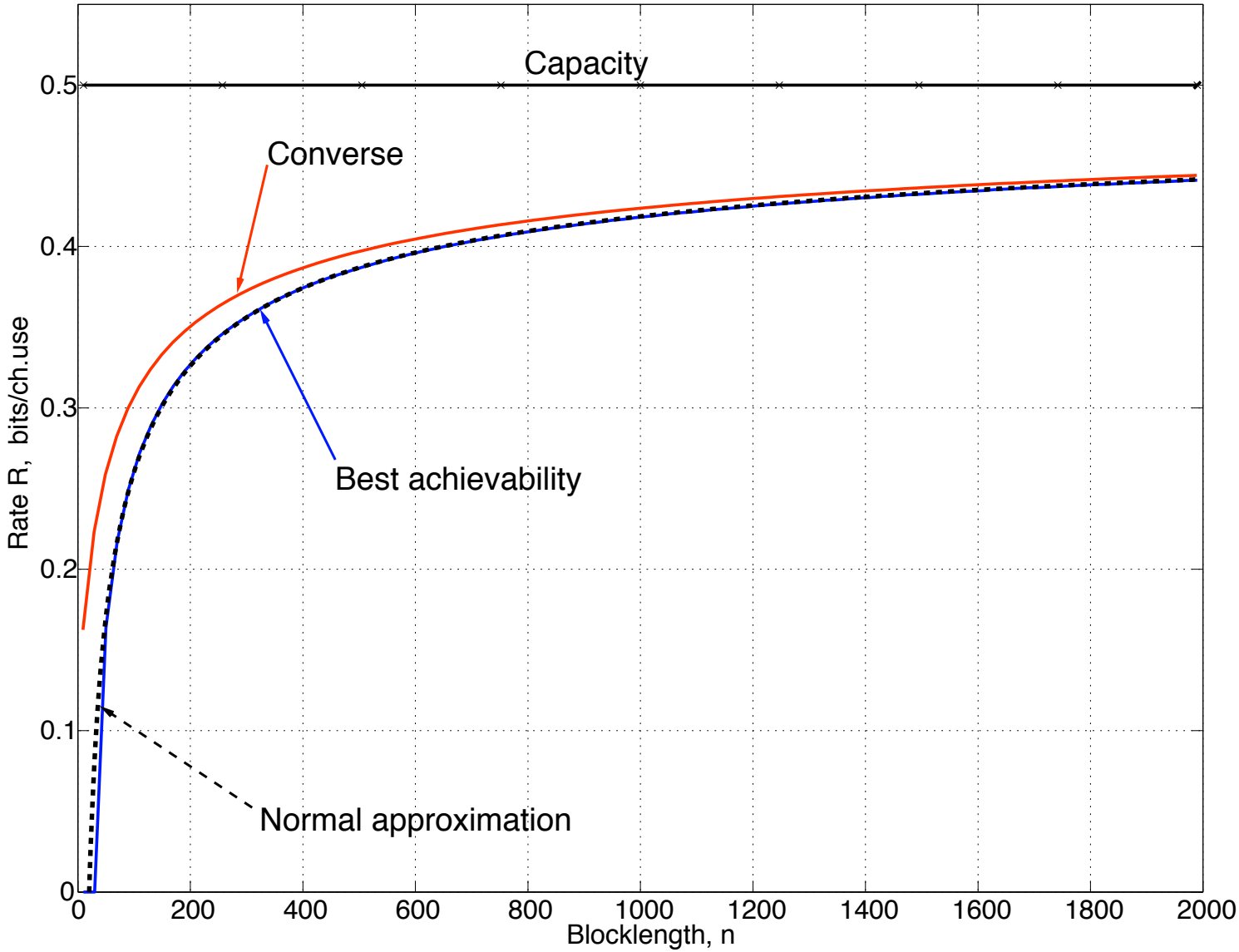
- (n,M,ε) code: $P(W \neq \hat{W}) \leq \varepsilon$
- Fundamental limit: $M^*(n,\varepsilon) = \max\{M: \exists \text{ an } (n,M,\varepsilon) \text{ code}\}$

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

$C = \mathrm{E}[i(X^*,Y^*)]$ (Shannon's capacity); $V = \mathrm{Var}[i(X^*,Y^*)]$ ("dispersion")

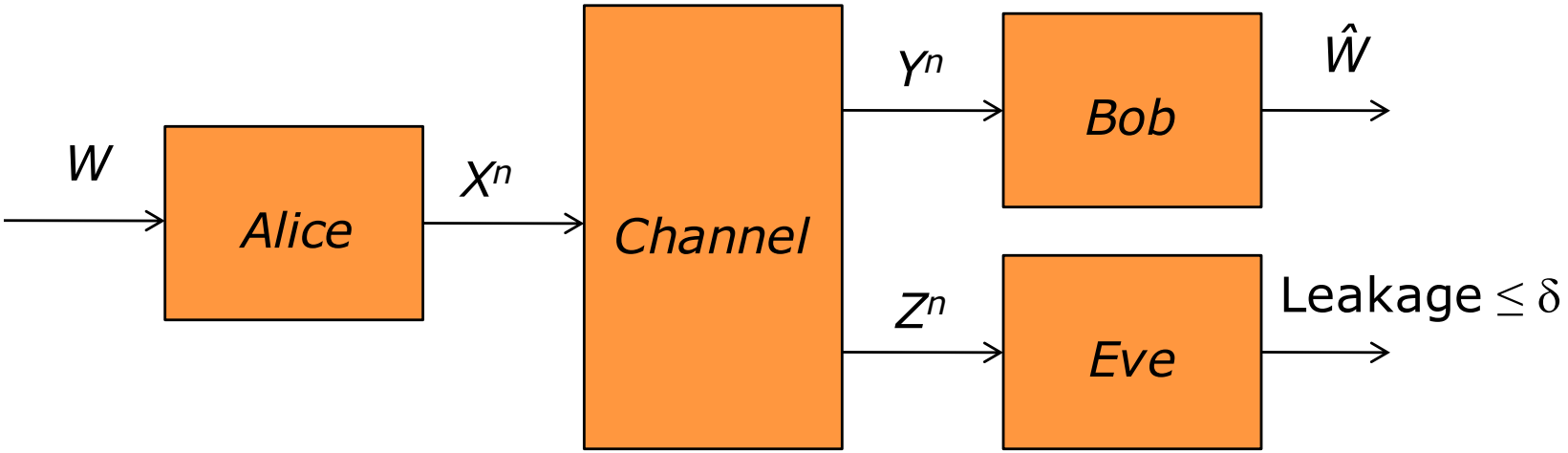
[Polyanskiy, et al. IT'10, etc.]

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



[Polyanskiy, et al. (2010)]

PHY Layer Security: Finite Blocklength



- (M, ϵ, δ) secrecy code:
  - Message $W \in \{1, \ldots, M\}$
  - Encoder $P_{X|W} : \{1, \ldots, M\} \to \mathcal{A}$; decoder $g : \mathcal{B} \to \{1, \ldots, M\}$
  - Average error probability: $\mathbb{P}\left(W \neq \hat{W}\right) \leq \epsilon$
  - Secrecy constraint: information leakage $\leq \delta$

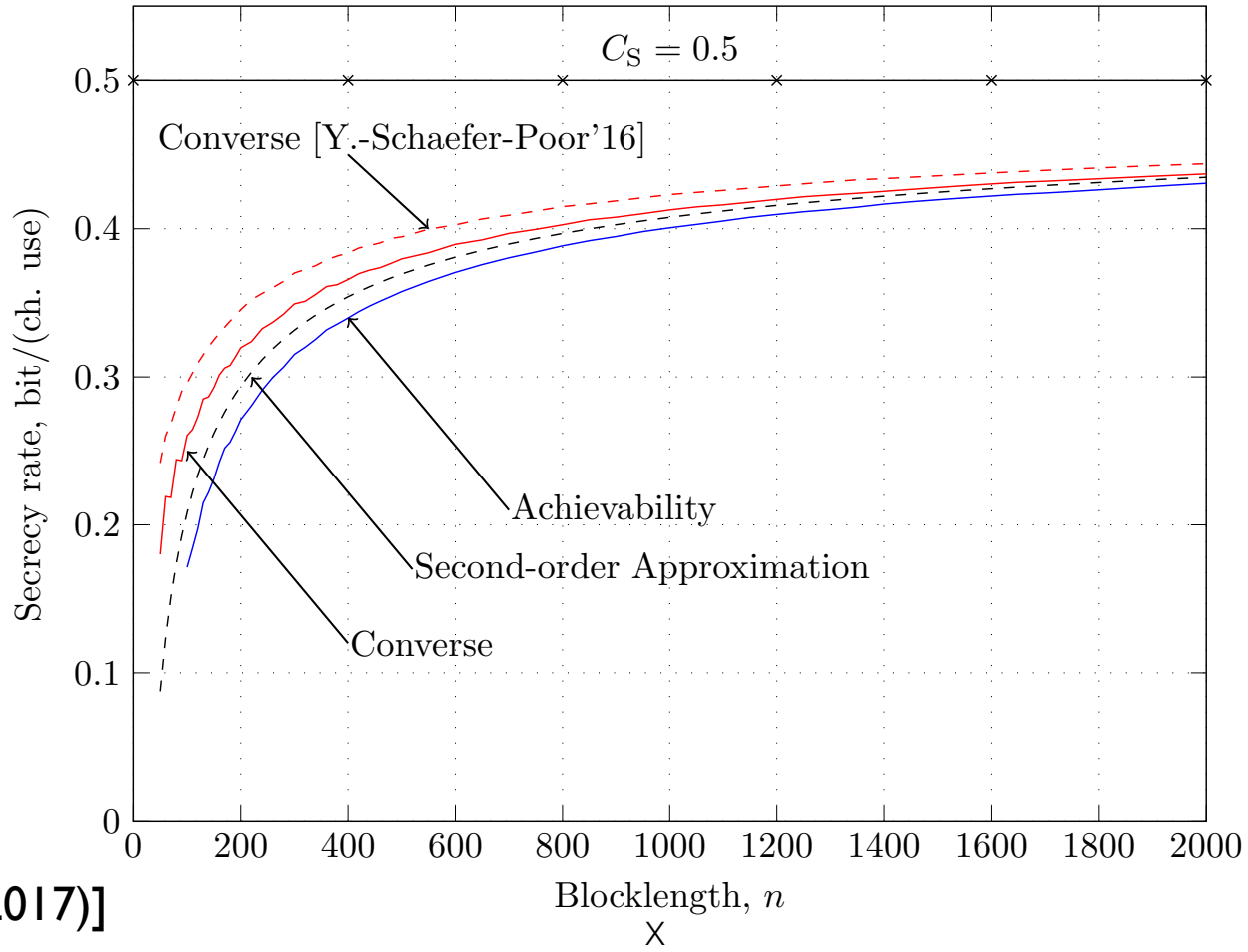
- $R^*(n, \epsilon, \delta)$: maximum secret rate at a given blocklength.

[Yang, Schaefer, Poor, IT'19]

Semi-deterministic Wiretap Channel (BSC): $\delta = \epsilon = 10^{-3}$

- Legitimate channel is deterministic, eavesdropper channel is BSC:

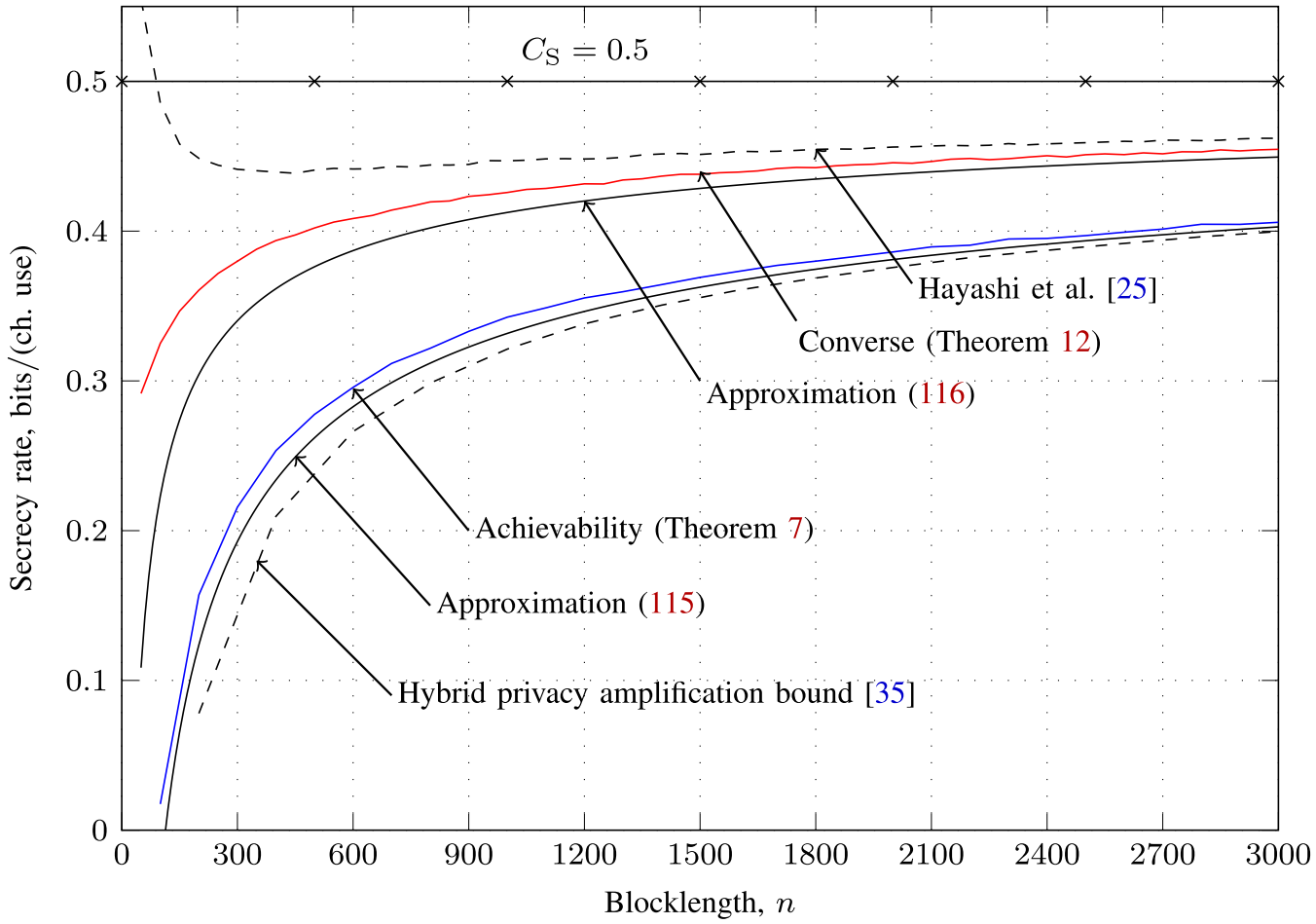
$$R^*(n, \epsilon, \delta) = C_s - \sqrt{\frac{V}{n}} Q^{-1}\left(\frac{\delta}{1-\epsilon}\right) + \mathcal{O}\left(\frac{\log n}{n}\right)$$



[Yang, et al. (2017)]

Gaussian Wiretap Channel

(SNR_{Bob} = 3db; SNR_{Eve} = - 3db)



[Yang, Schaefer, Poor, IT'19]

Key Generation from Common Randomness

- Passive Eavesdropper:
  - Public discussion
  - Channel reciprocity: joint source-channel model
  - Relay assisted: trusted or oblivious
- Active Eavesdropper:
  - Channel reciprocity: joint source-channel model

Lai, Liang, Du, Poor (2015)
Key Generation from Random Channels
in *Physical Layer Security in Wireless Communications* (CRC)

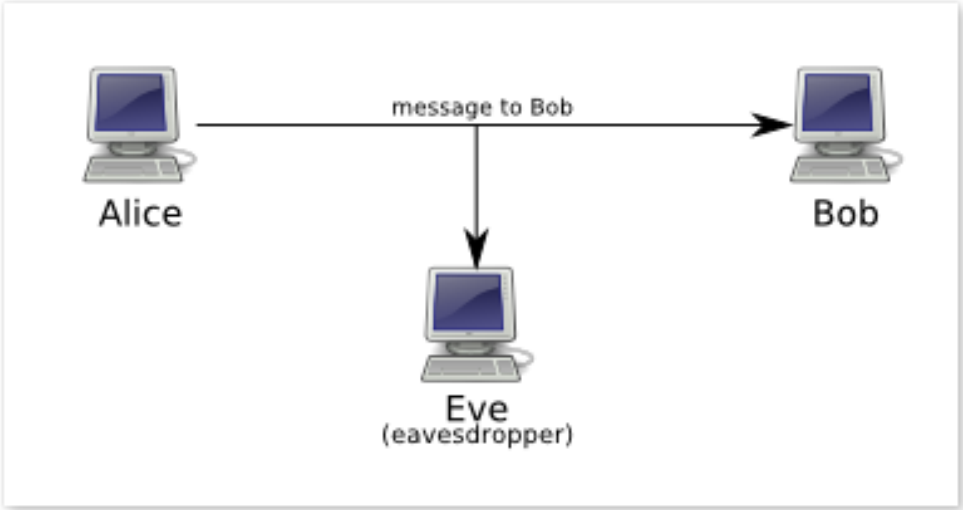
Privacy-Utility Tradeoffs

in

Sensing Systems

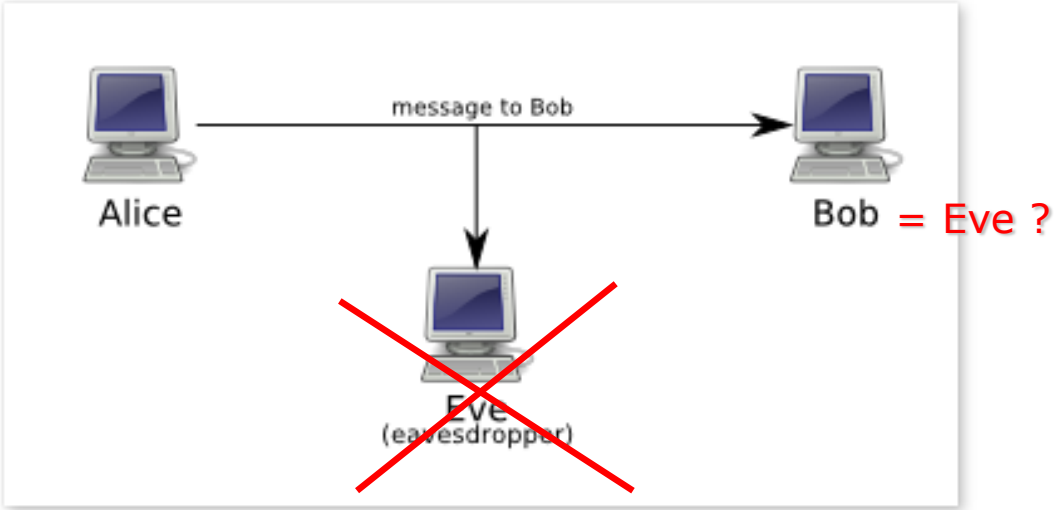
Privacy vs. Secrecy

- Privacy is not secrecy:



Privacy vs. Secrecy

- Privacy is not secrecy:

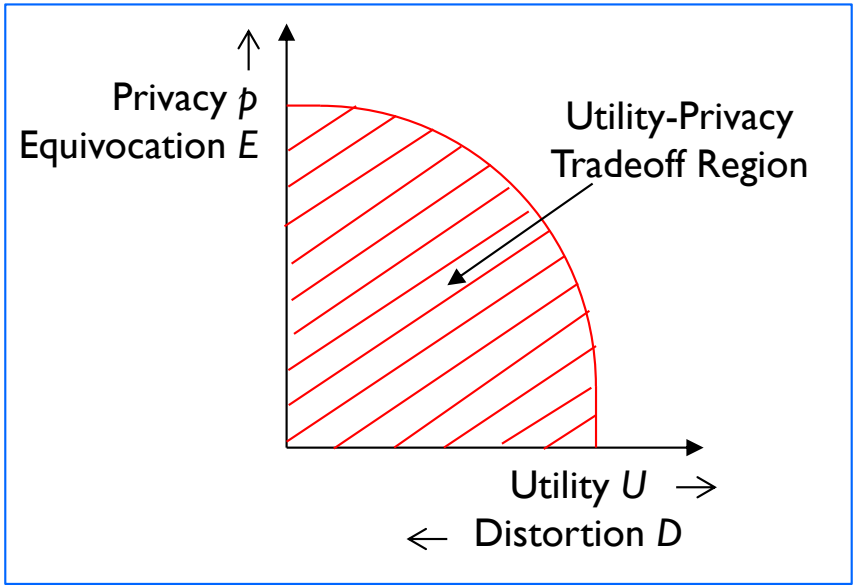


- Denial of access (secrecy) makes a data source useless.

Privacy-Utility Tradeoff

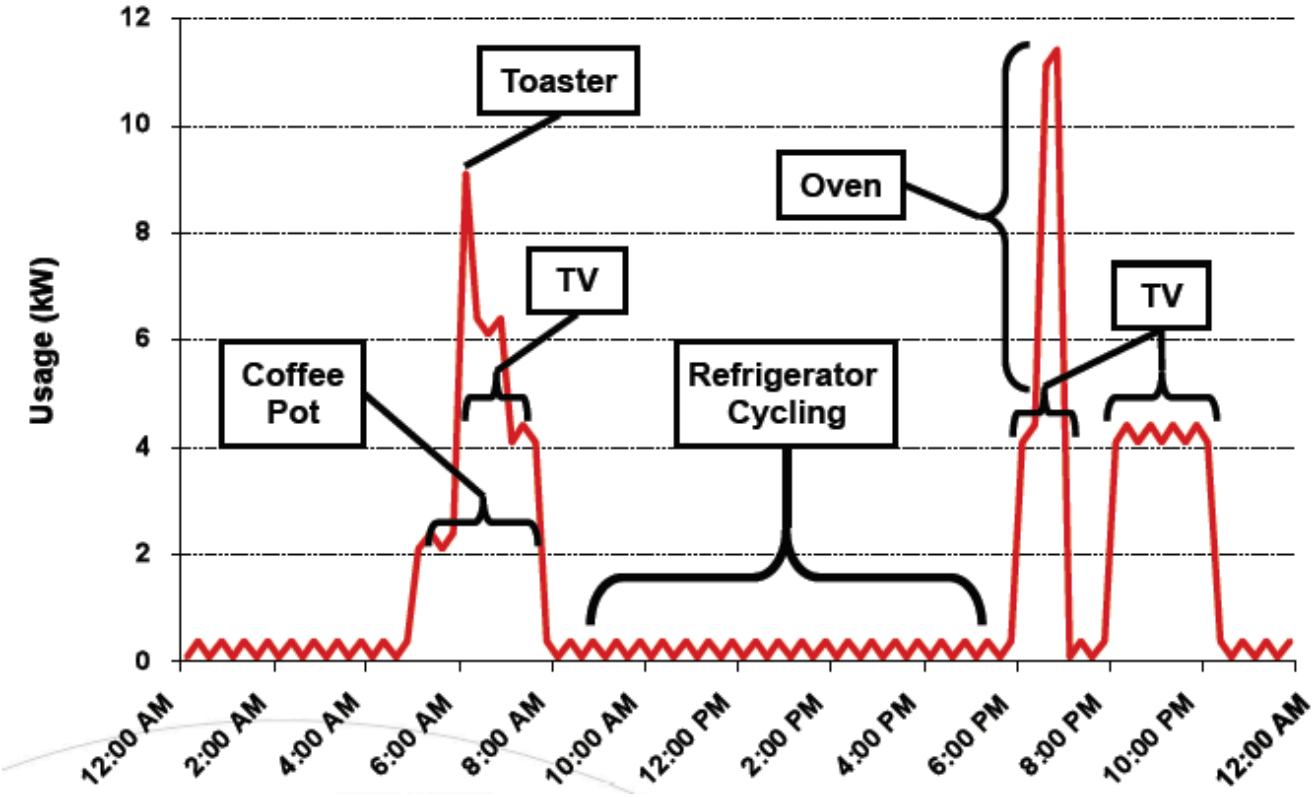
- Sensing systems generate considerable electronic data:

- Data's utility depends on its accessibility.
- Accessibility endangers privacy.
- This fundamental tradeoff can be characterized via information theory.



Example: Smart Meter Privacy

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

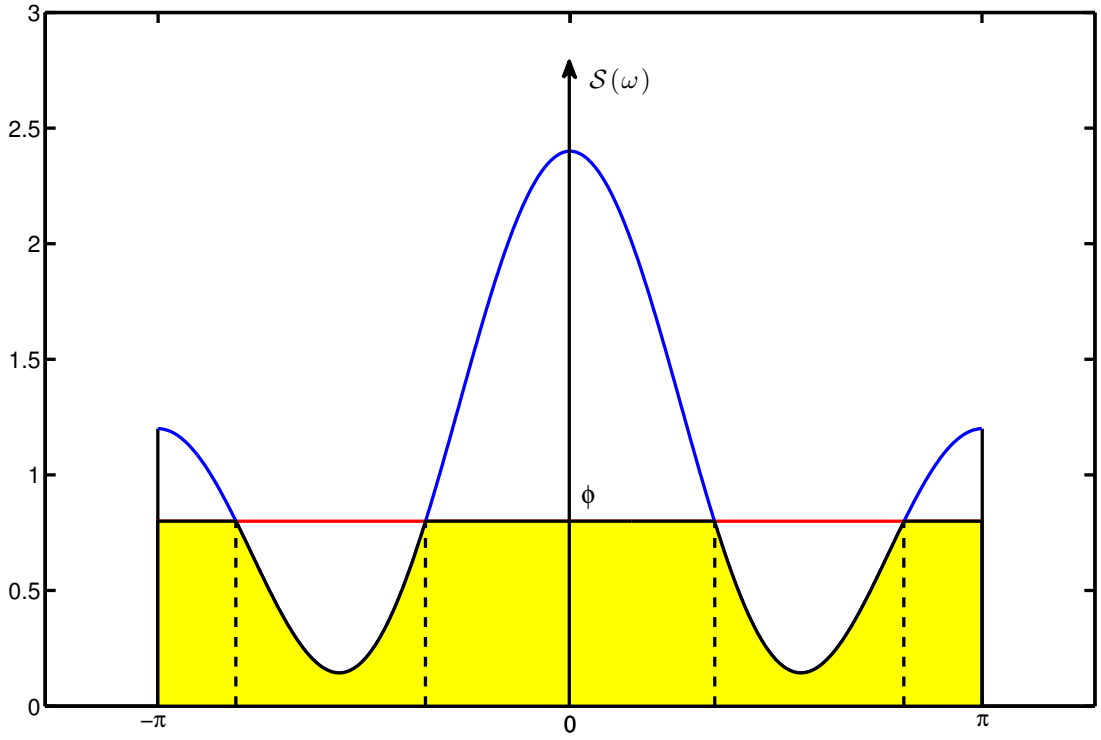


Giaconi, Gunduz, Poor (2021) Smart Meter Privacy, in *Advanced Data Analytics for Power Systems* (Cambridge)

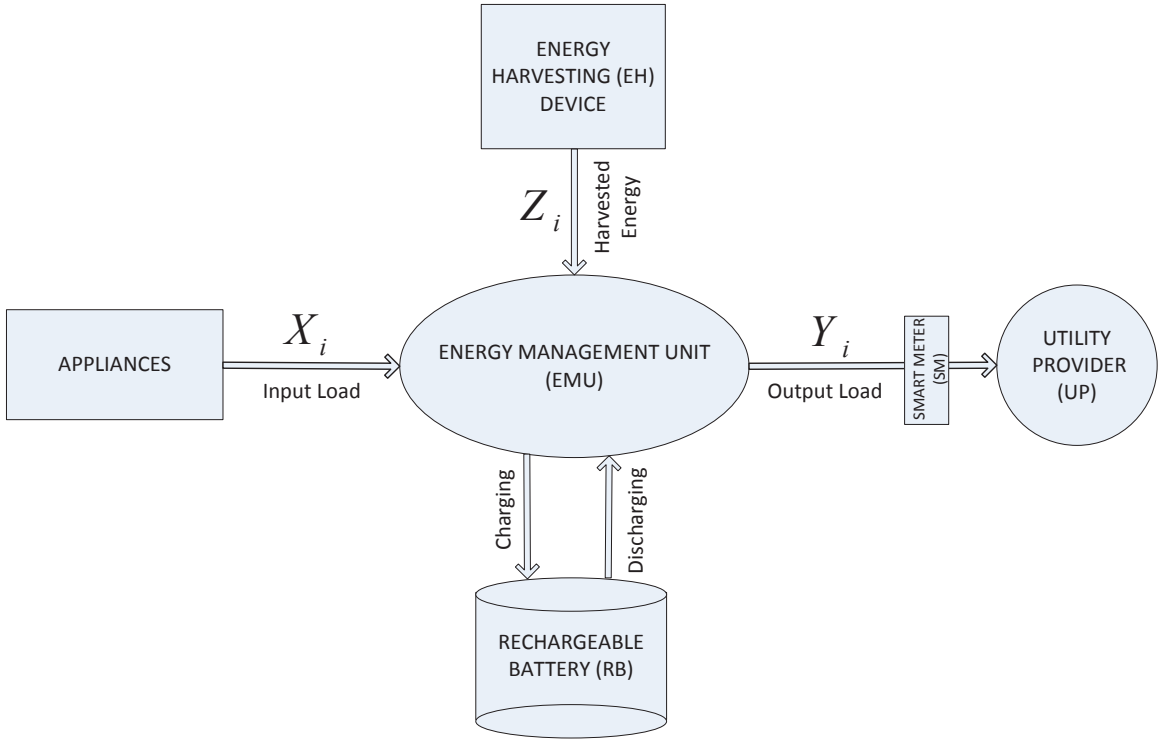
Source Coding Solution:

Hidden Gauss-Markov Model (protection of the hidden intermittency state)

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

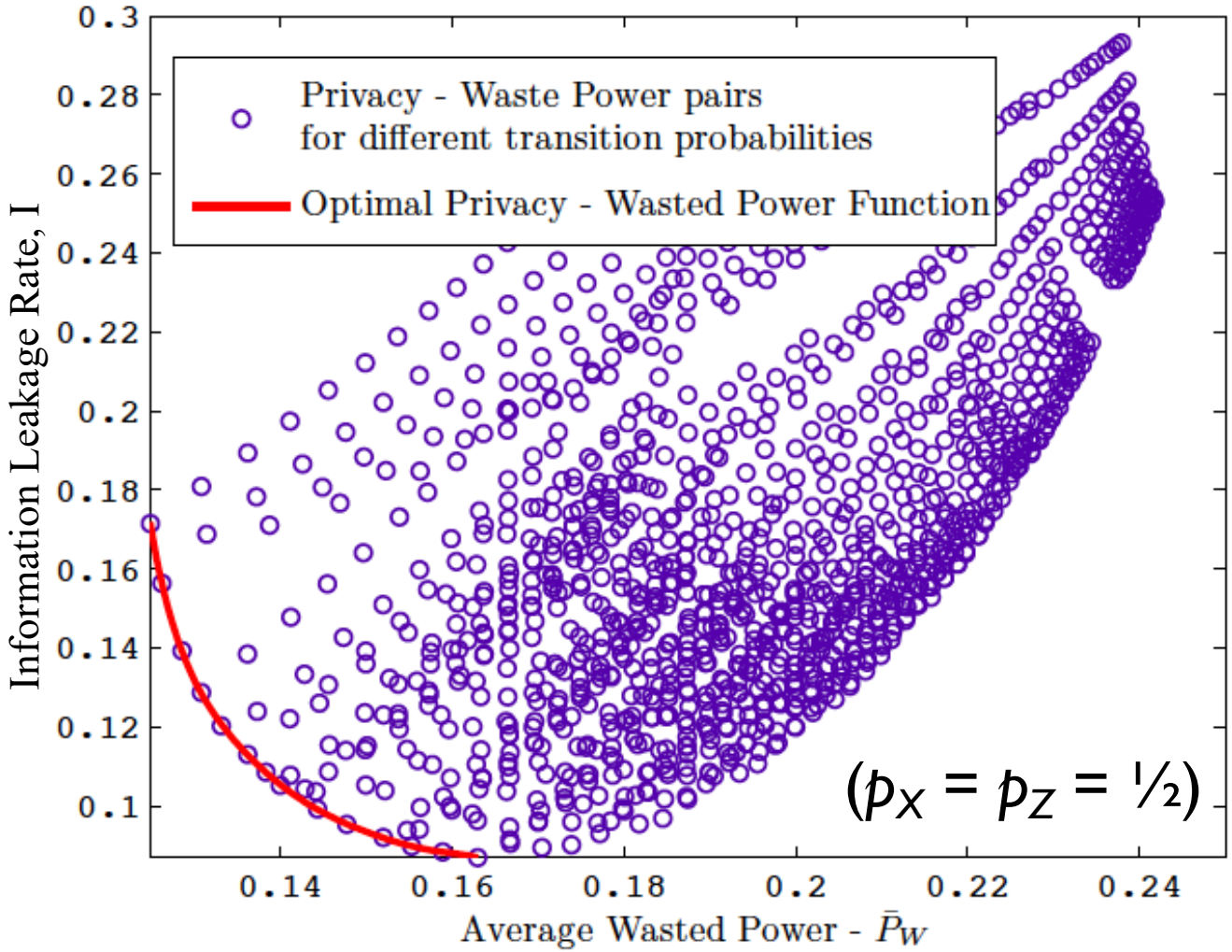


A Control Approach:
Energy Harvesting and Storage



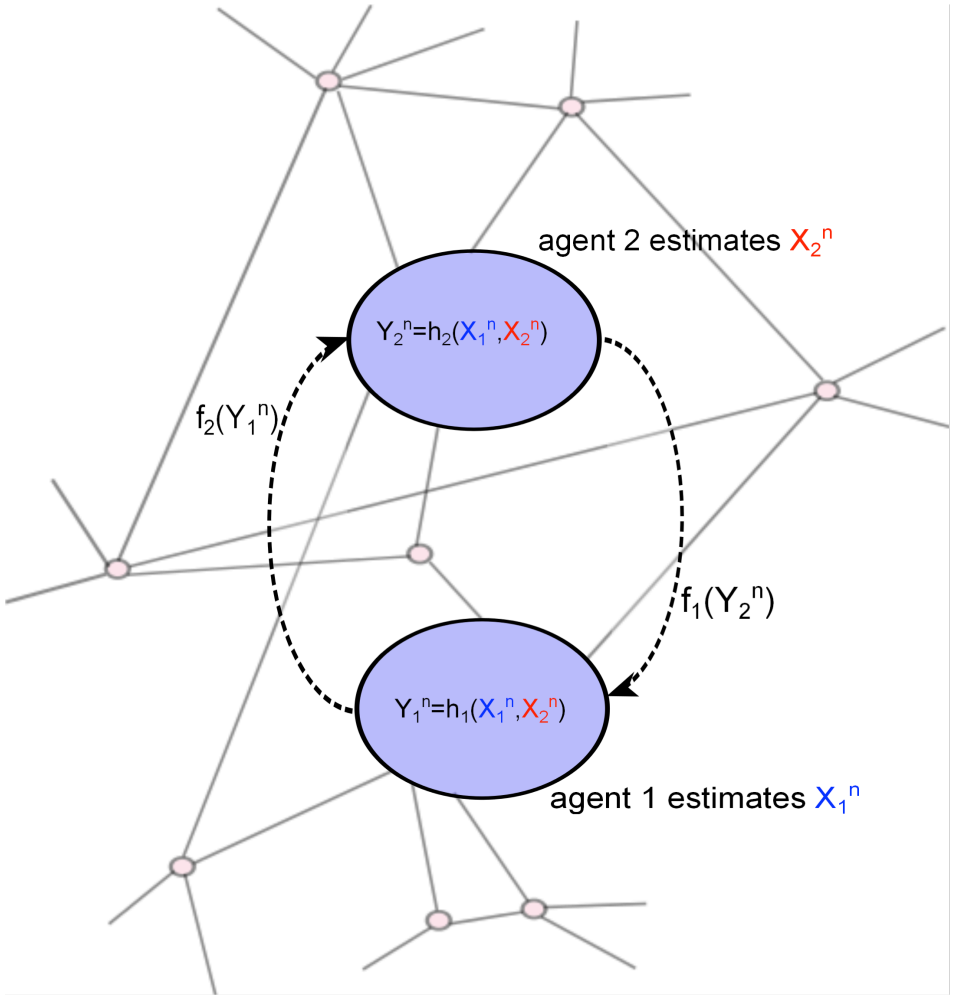
Tradeoff: wasted energy versus information leakage

Privacy-Utility Tradeoff:
Binary Variables



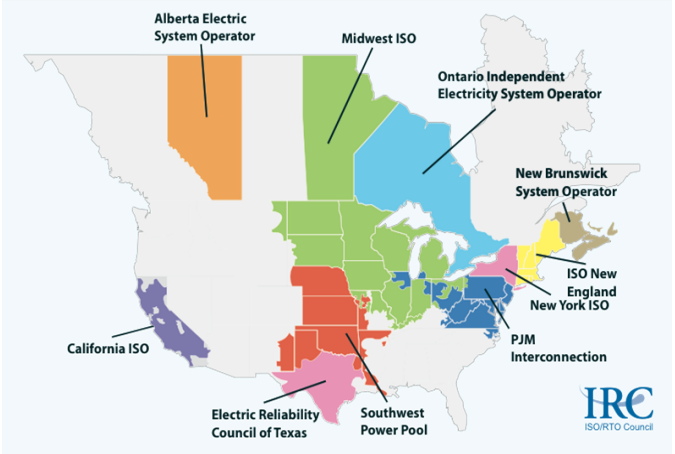
Competitive Privacy: Privacy-Utility Tradeoffs for Interacting Agents

- Multiple interacting, but competing, agents (or groups of agents) with coupled measurements.
- Each wants to estimate its own parameters, or state.
- They can help each other by sharing data, but wish to preserve privacy.
- Each has a privacy-utility tradeoff, but they are competitive ones.
- How should they interact?



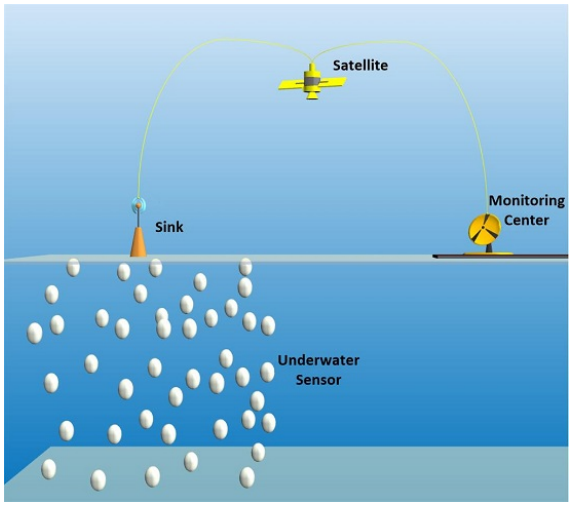
Motivating Examples

Electricity Grids:
grid management



Radar: untrustworthy allies

Sensor Networks:
resource localization

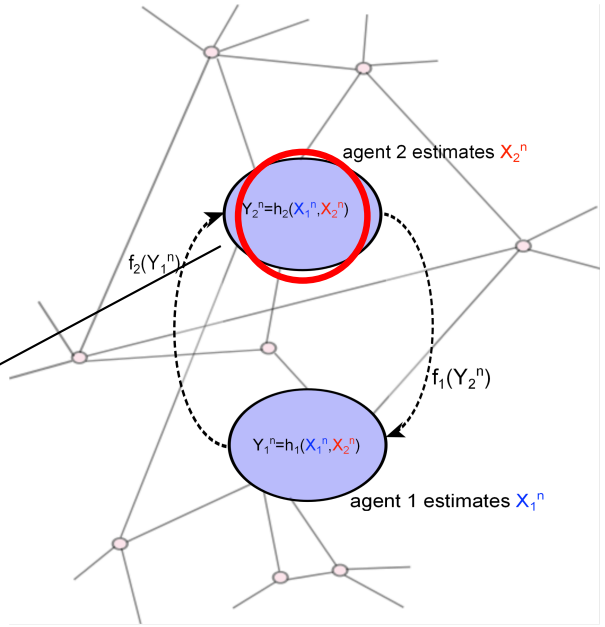


Linear Measurement Model

- Noisy measurements at agent k:

$$Y_k = \sum_{m=1}^{M} H_{k,m} X_m + Z_k, \; k = 1,2,\ldots,M$$

m^{th} system state

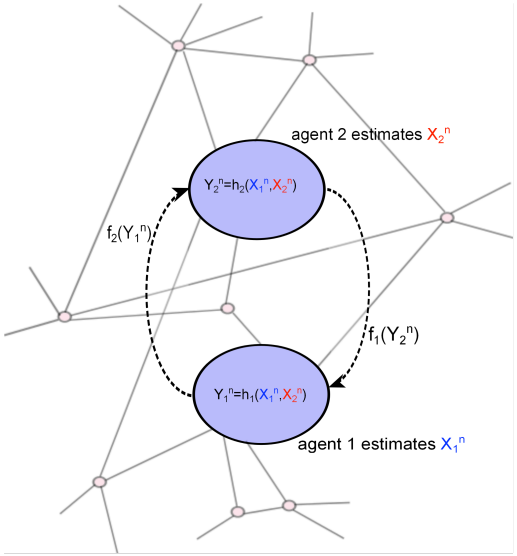


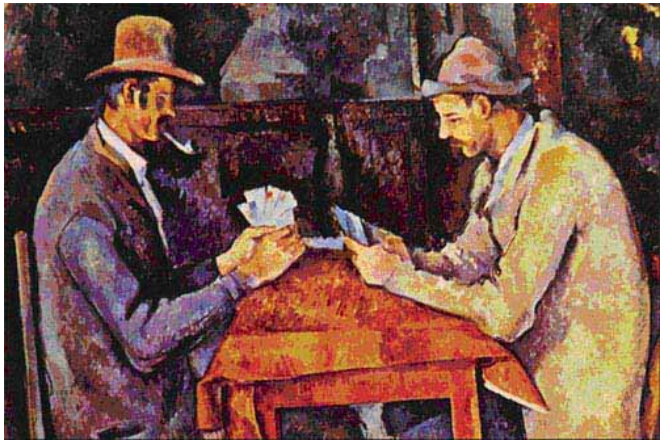
- Utility for agent k: mean-square error for its own state X_k

- Privacy for agent k: leakage of information about X_k to other agents

How Should Agents Exchange Data?

- This is a classical problem in information theory – the Wyner-Ziv problem (optimal distributed source coding) – which tells how to exchange information.
- But, doesn't say how much information to exchange.





- Because of the competitive nature, game theory or prospect theory can illuminate this.
- Leads to a number of interesting solutions:
  - a basic problem is a prisoners' dilemma
  - with pricing, cooperation or multi-play games, more meaningful solutions arise

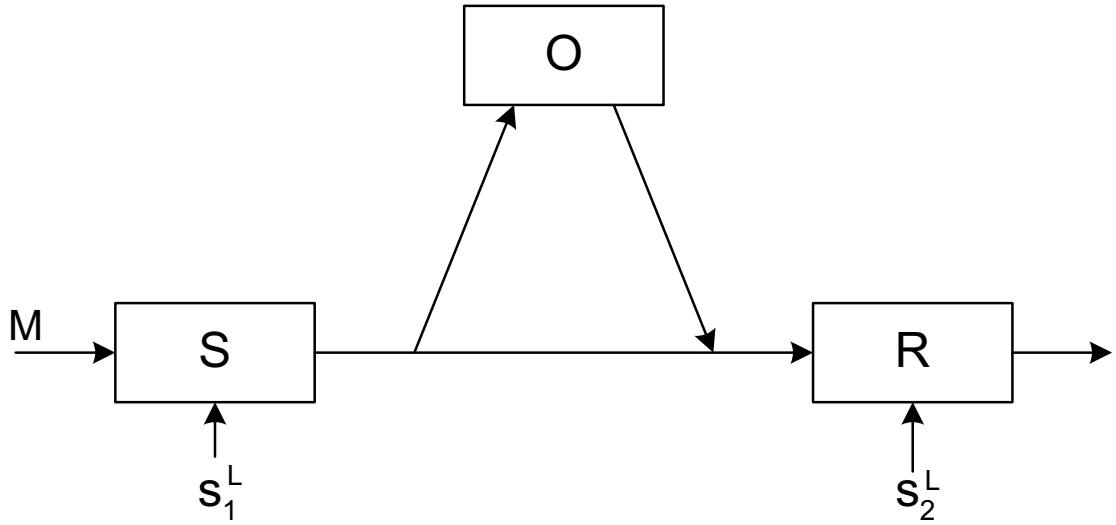
Poor (2018)
Privacy in Networks of Interacting Agents
in *Emerging Applications of Control and System Theory* (Springer)

Other Issues

Other Issues

- Authentication
  - Information theoretic bounds on the probabilities of successful impersonation and substitution attacks [Lai, et al. IT'09]
- Attacks on MANETs
  - Information theoretic guidance on how many malicious nodes can be tolerated [Liang, et al. IT'11]
- Man-in-the-Middle and Spoofing Attacks on Sensor Nets
  - Effects on CRLB in parameter estimation [Zhang, et al. SPM'18]

Authentication with Correlated Sequences



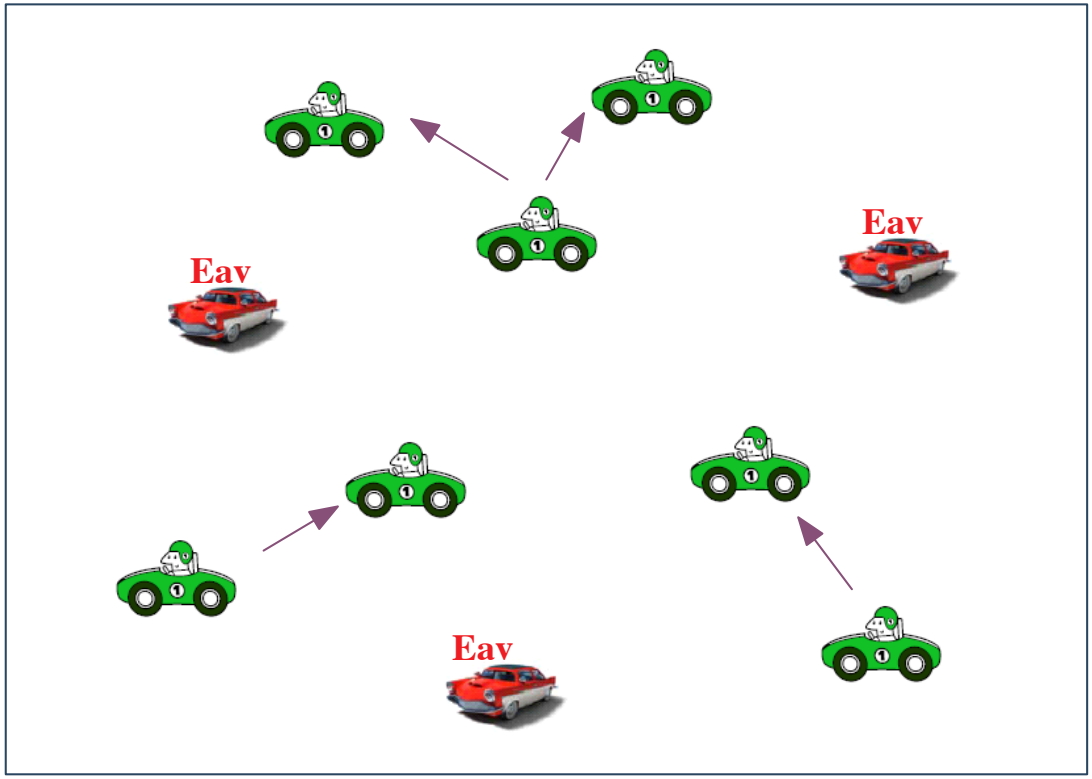
Impersonation attack: O transmits a message before S

Substitution attack: O replaces S's message with its own

Theorem [Lai, et al. IT'09]: If the S-O channel is not less noisy than the S-R channel, then

$$P_I = P_S = 2^{-LI(S_1;S_2)}$$

MANETs with Malicious Nodes



- n legitimate mobile nodes
- Each legitimate node is both a source and a destination.
- m malicious nodes

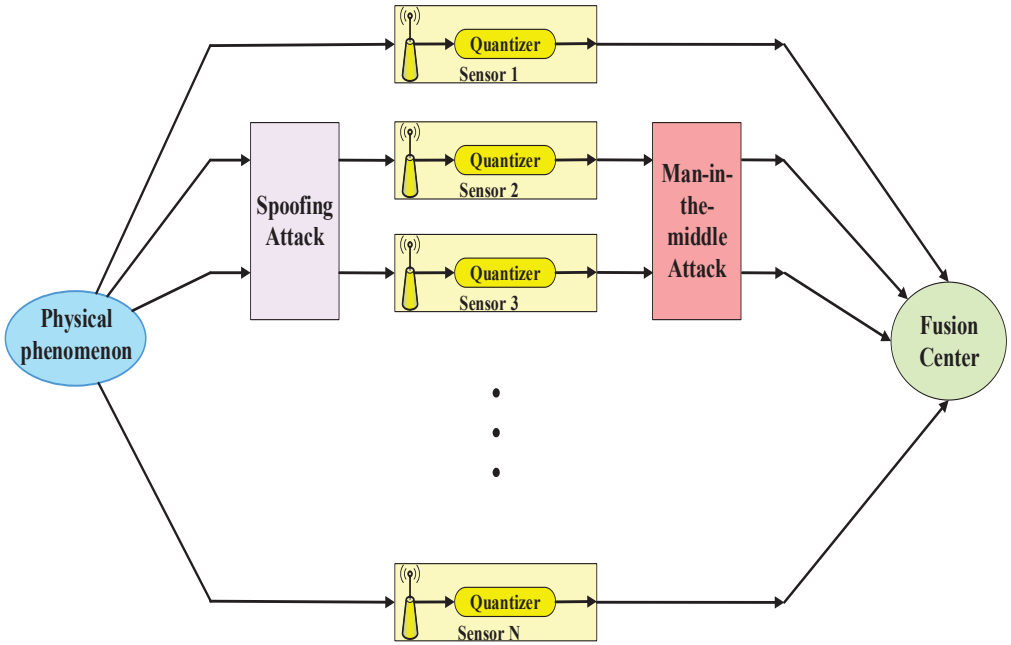
Secrecy Capacity Scaling

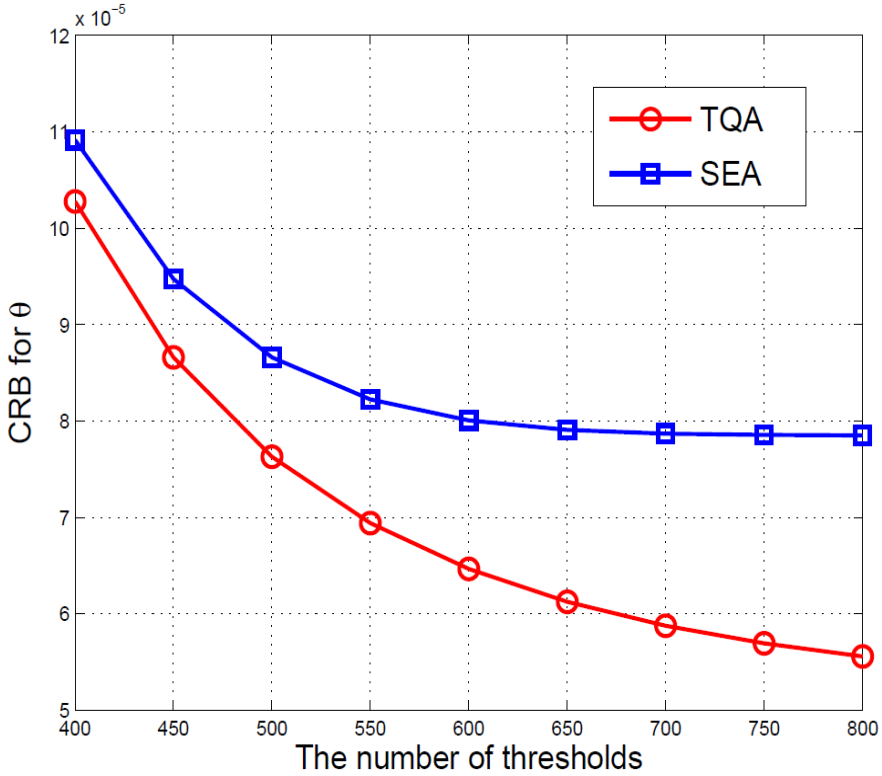
[Liang, et al. IT'11]

- Case I: $m = o(\sqrt{nD})$
  - # of malicious nodes is small
  - Type II packets (two-hop scheme) dominate
  - $C_s = \Theta\left(\sqrt{\frac{D}{n}}\right)$
  - Presence of malicious nodes has negligible impact
- Case II: $m = \Omega(\sqrt{nD}poly(n))$
  - # of malicious nodes is large
  - Type I packets (one-hop scheme) dominate
  - $C_s = \Theta\left(\frac{1}{m}\right)$
  - Secrecy throughput is determined by # of malicious nodes

Attacks on Sensor Nets

[Zhang, et al. SPM'18]





Man-in-the-middle attack:

- TQA uses attacked data
- SEA ignores attacked data

Closing Thoughts

- Information theory can help understand some fundamental limits of security and privacy in wireless networks

- These are theoretical constructs; although they sometimes point to potential practical solutions, there are many needs to connect this kind of analysis to real networks, e.g.
  - more finite-blocklength analysis
  - scaling laws for large networks
  - practical coding schemes to achieve fundamental limits
  - other security primitives (signatures, certificates, etc.)

- Not all security has to be iron-clad: Quality of Security can be a parameter, just like Quality of Service

Some References

Schaefer, Boche, Khisti, Poor (2017) *Information Theoretic Security and Privacy of Information Systems* (Cambridge)

Poor, Schaefer (2017) Wireless Physical Layer Security, PNAS.

Poor (2018) Privacy in Networks of Interacting Agents, in *Emerging Applications of Control and System Theory* (Springer)

Yang, Schaefer, Poor (2019) Wiretap Channels: Nonasymptotic Fundamental Limits, *IEEE Transactions on Information Theory*

Yagli, Dytso, Poor (2020) Information-Theoretic Bounds on the Generalization Error and Privacy Leakage in Federated Learning, *Proceedings SPAWC*

Giaconi, Gunduz, Poor (2021) Smart Meter Privacy, in *Advanced Data Analytics for Power Systems* (Cambridge)

Herfeh, Chorti, Poor (2021) Physical Layer Security: Authentication, Integrity and Confidentiality, in *Physical Layer Security* (Springer)

Thank You!