Fundamentals of IoT Networks

Secure and Low Latency Communications

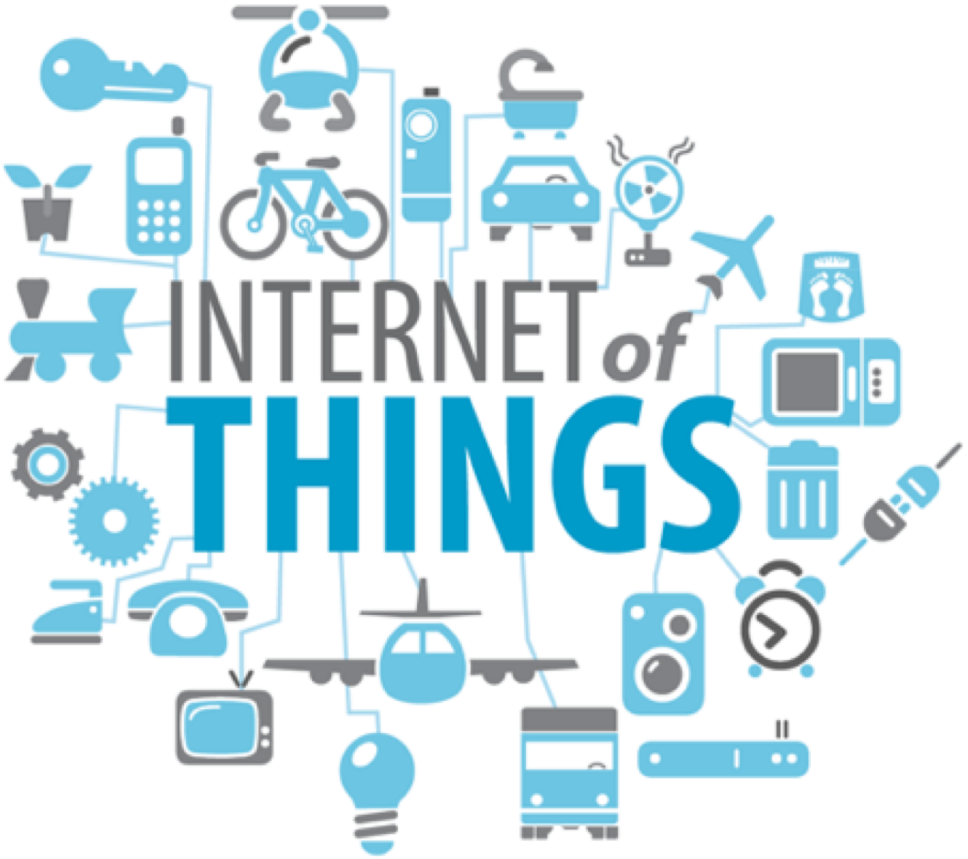
H. Vincent Poor
(poor@princeton.edu)

Supported in part by NSF Grants CCF-0939370 and CCF-1513915.

The Internet of Things (IoT) Vision

Salient Characteristics of the IoT

- Massive connectivity
- High energy efficiency
- Low complexity
- Light infrastructure
- Short packets
- Low latency



- Primary applications are sensing, inference and control

Overview of Today's Talk

The theme:

- The need for new fundamentals

Two topics motivated by the characteristics of IoT:

- Latency: finite-blocklength information theory +
- Security: physical layer issues (briefly)

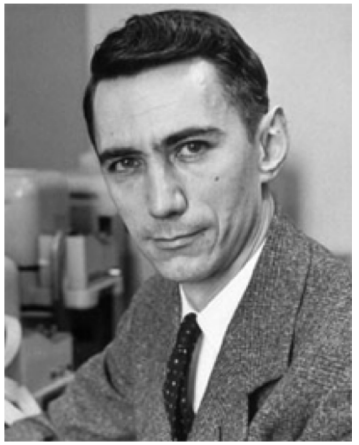
Latency:

Finite-Blocklength

Information Theory +

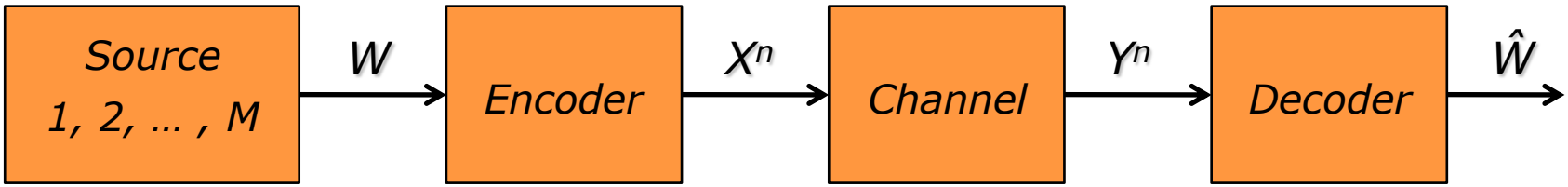
Traditional Information Theory

- Benefit
  - Characterizes operational, engineering problems in terms of elegant mathematical formulas



- An asymptotic theory
  - Fundamental limits asymptotic in the blocklength
- Limitation
  - Not suitable for low-latency applications as in IoT

Finite Blocklength IT: Data Transmission



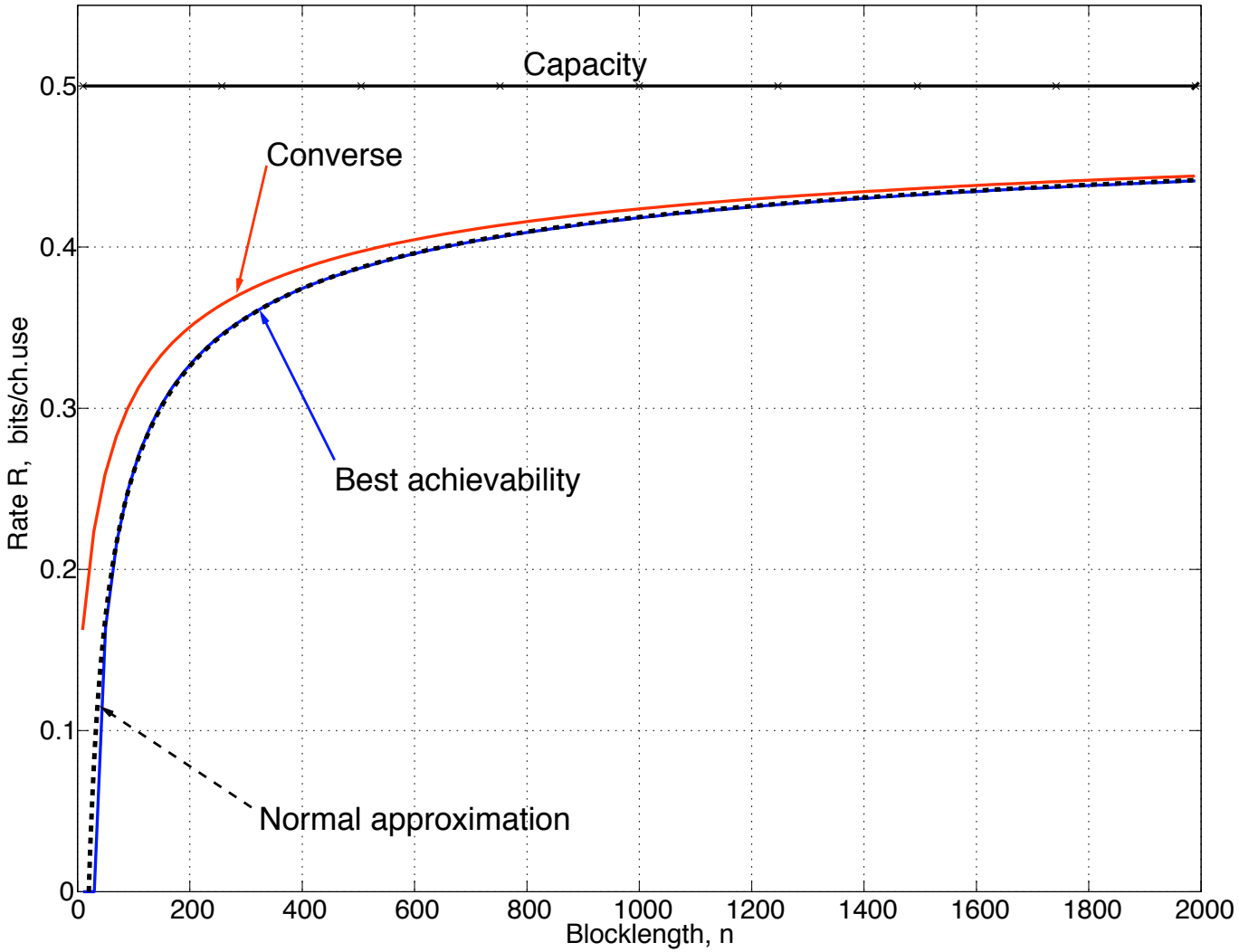
- (n,M,ε) code: $P(W \neq \hat{W}) \leq \varepsilon$
- Fundamental limit: $M^*(n,\varepsilon)$ = max{M: $\exists$ an (n,M,ε) code}

$$R^*(n,\varepsilon) \approx \frac{\log M^*(n,\varepsilon)}{n} = C - \sqrt{\frac{V}{n}}\, Q^{-1}(\varepsilon)$$

C = E[$i(X^*,Y^*)$] (capacity); V = Var[$i(X^*,Y^*)$] ("dispersion")

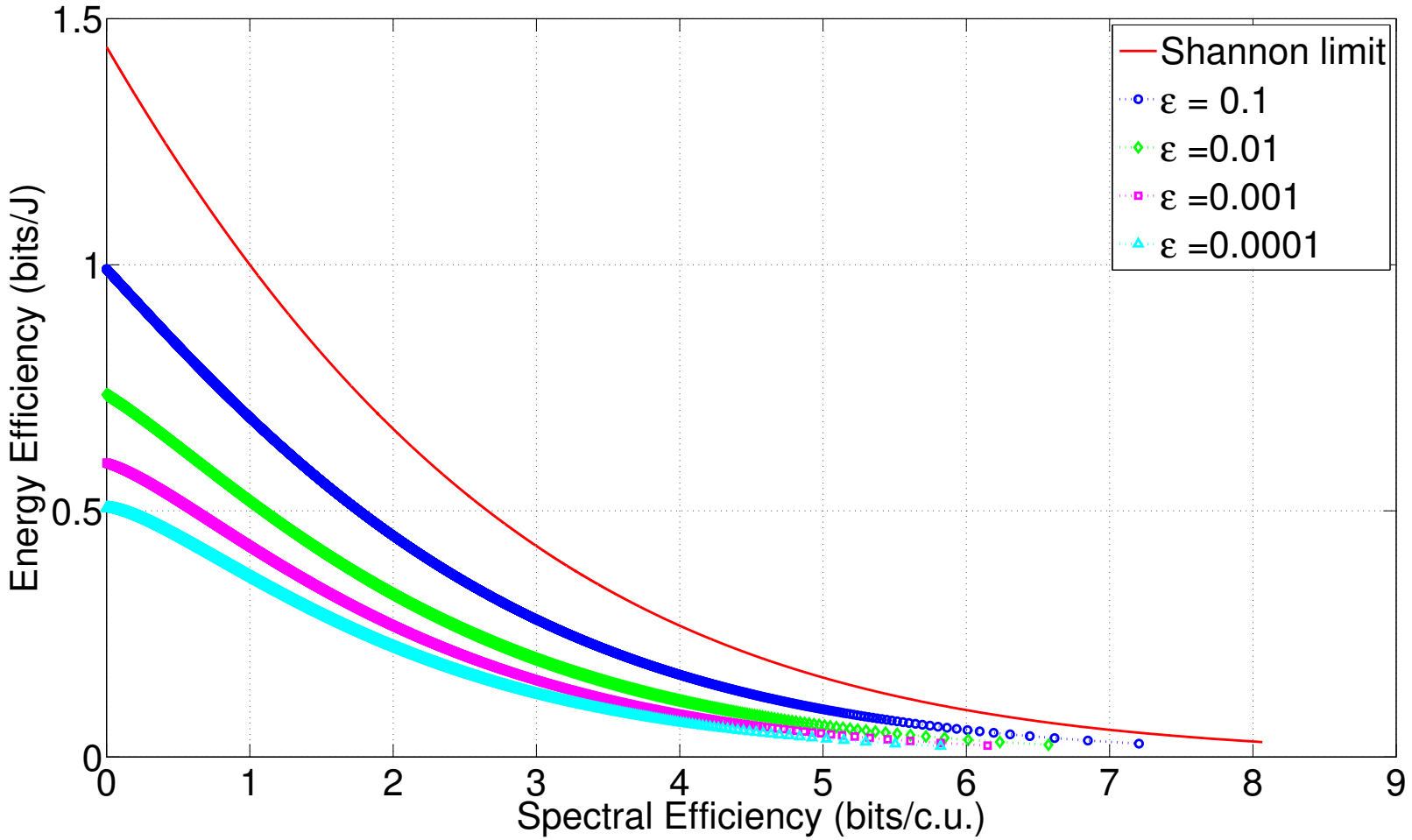
[Polyanskiy, et al. (2010), etc.]

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



[Polyanskiy, et al. (2010), etc.]

Example: Spectral-Energy Efficiency Tradeoff



[Gorce, et al. (2016)]

Finite-Blocklength Compression

rate-distortion function

rate-dispersion function

Lossy:

$$R(n,d,\epsilon) \approx R(d) + \sqrt{\frac{V(d)}{n}} Q^{-1}(\epsilon)$$

probability the distortion exceeds *d*

[Kostina, et al. (2012)]

entropy

varentropy

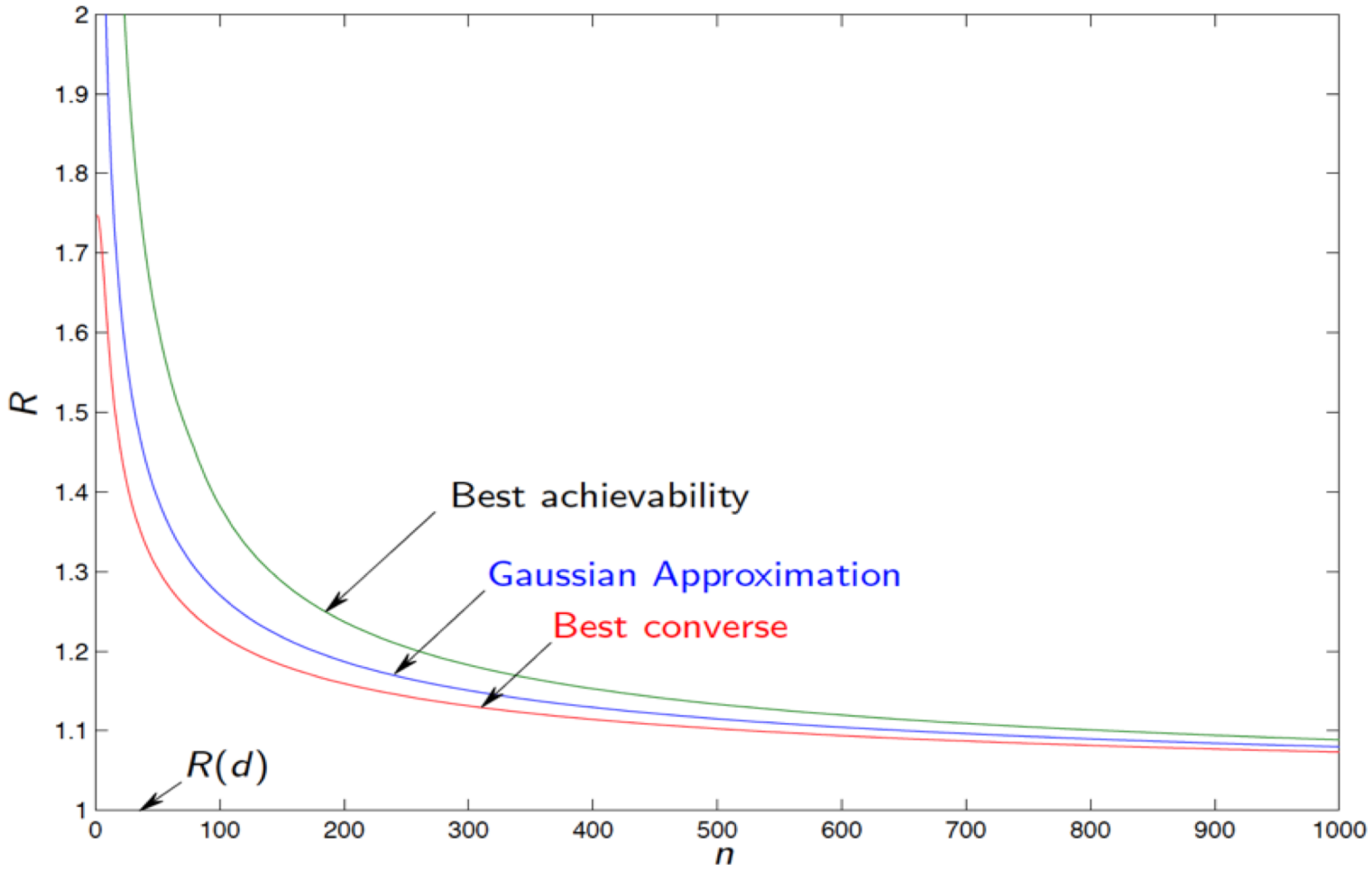
Lossyless:

$$R^{\star}(n,\epsilon) \approx H(X) + \sqrt{\frac{\sigma^2(X)}{n}} Q^{-1}(\epsilon)$$

encoding failure probability

[Kontoiannis, et al. (2014)]

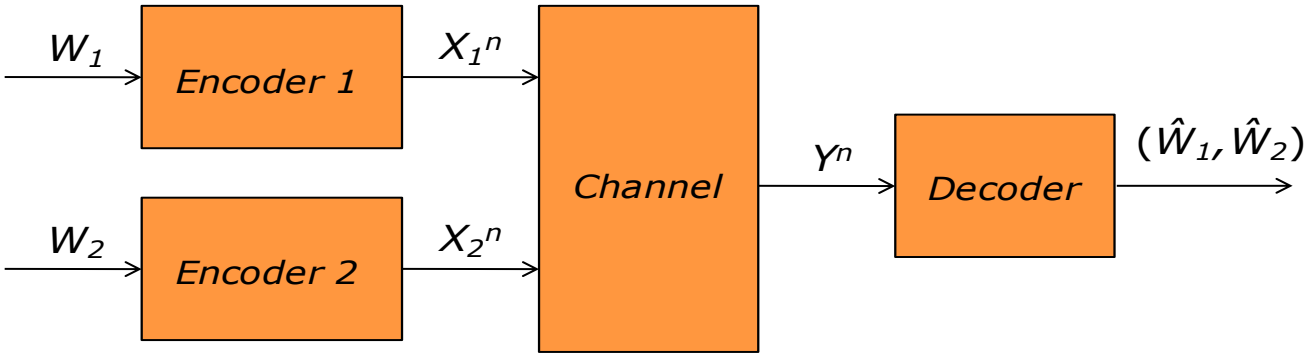
Ex: Memoryless N(0,1) Source $d = 1/4$; $\varepsilon = 10^{-4}$



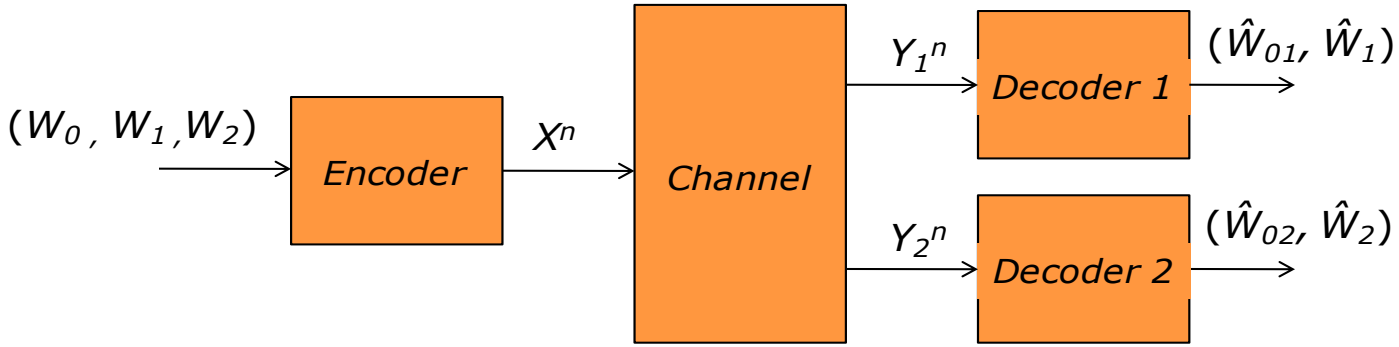
[Kostina, et al. (2012)]

Prototype Network Models

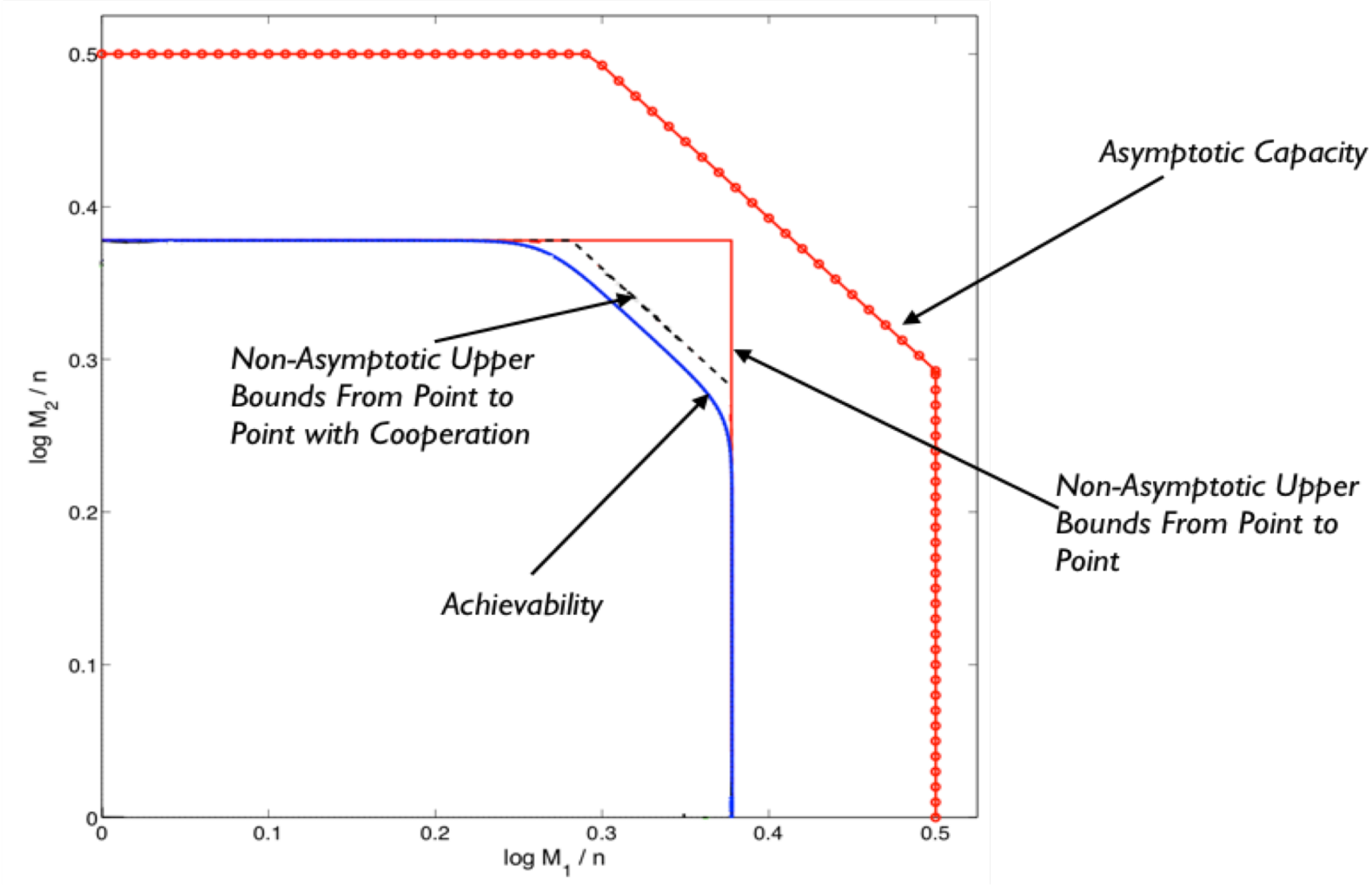
Multiple-Access Channel ("Uplink"): [MolavianJazi, et al. (2013)] [Scarlett, et al. (2015)]



Broadcast Channel ("Downlink"): [Liu, et al. (2015)]



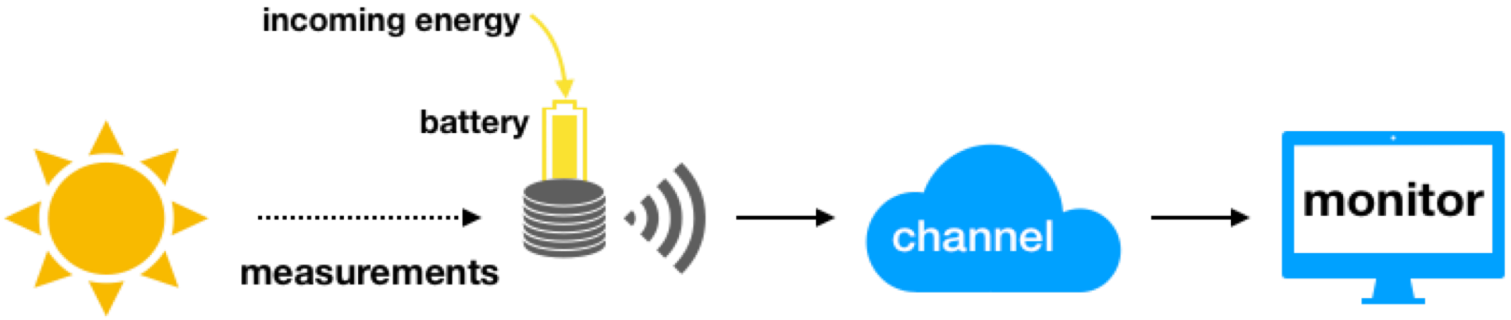
Example: Gaussian MAC Rate Region: $n = 500$; equal powers of 0dB; $\varepsilon = 10^{-3}$



[MolavianJazi, et al. (2013)]

Other Approaches to Assessing Latency

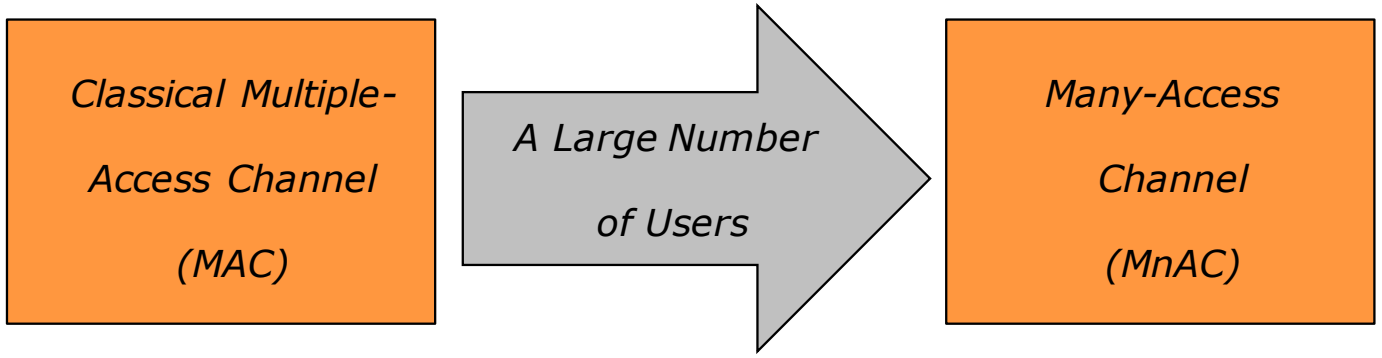
Age of Information (AoI):



- AoI: time since latest measurement has reached destination
- Assesses the freshness of data, in addition to distortion/error
- Suitable metric for real-time sensing applications in IoT

Other Approaches to Assessing Latency

The Many-Access Channel:



The number of users *K(n)* is fixed as the blocklength *n* goes to infinity.

The number of users *K(n)* increases with the blocklength *n*.

Main Ideas:

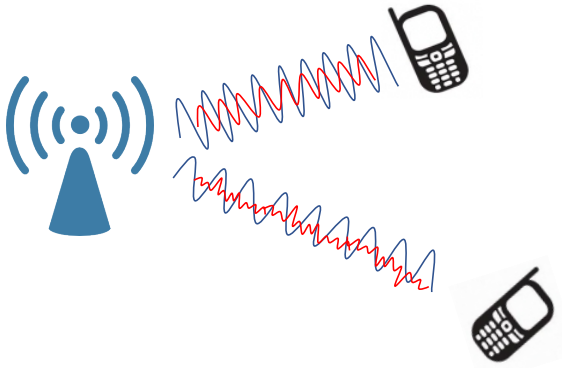
- Blocklength is proportional to latency
- System latency per user $\ell = \dfrac{n}{K(n)}$
- There's a tradeoff between system rate and latency

Security:

Physical Layer Issues

(Briefly)

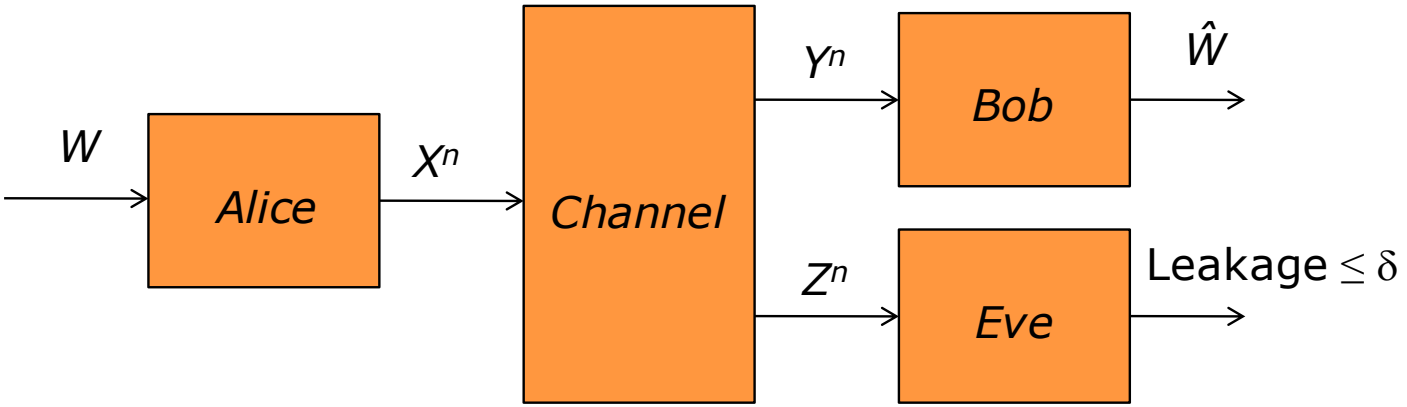
Rethinking Security Design



- Conventionally, a higher layer issue: encryption, key distribution, …
- Difficult with massive number of devices, light infrastructure, low complexity, …
- Physical layer security provides a degree of security by exploiting imperfections in physical channels: noise, fading, …

Wyner's Model for Data Confidentiality

"The Wiretap Channel"



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

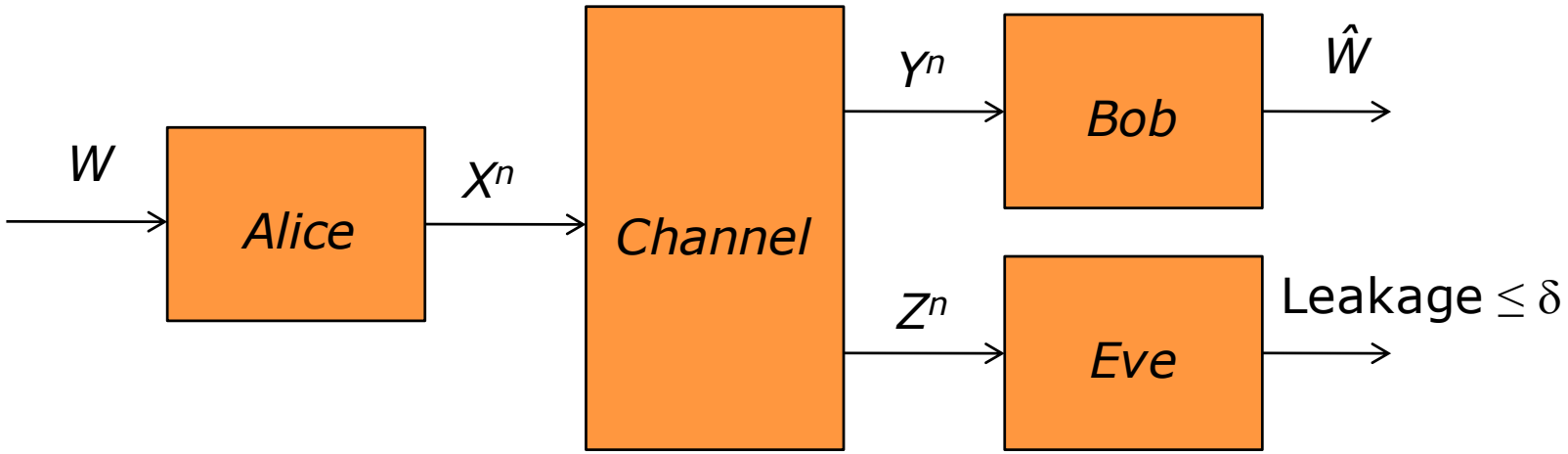
Physical Layer Security: Data Confidentiality

- 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

[Poor, Schaefer (2017) Wireless Physical Layer Security PNAS]

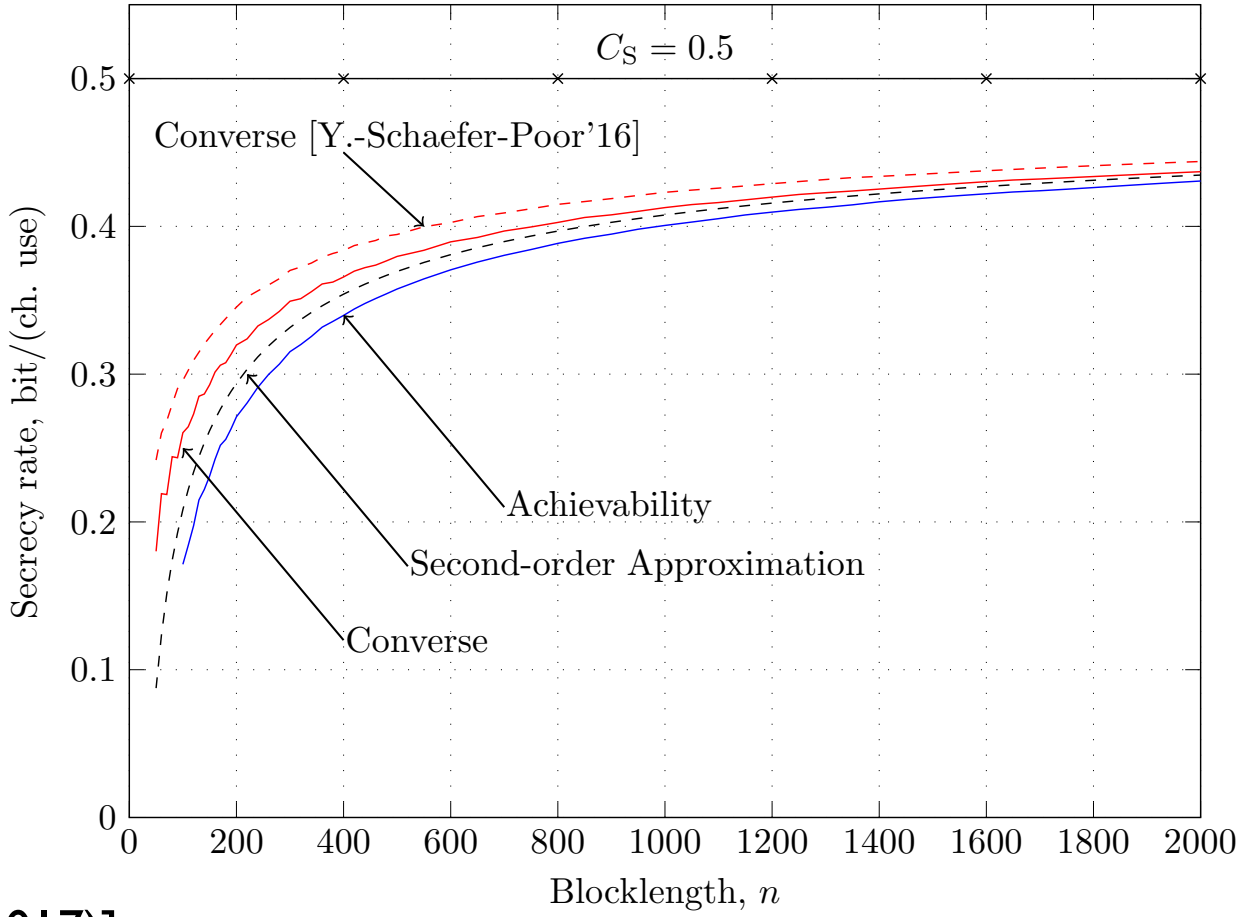
Wiretap Channel for Finite Blocklength



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

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

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



[Yang, et al. (2017)]

Other PHY Security Issues in IoT

- Authentication
  - Probability of successful impersonation/substitution attacks [Lai, et al. (2009)]
- Attacks on MANETs
  - How many malicious nodes can be tolerated? [Liang, et al. (2011)]
- Data Injection Attacks on Smart Grids
  - Protection against stealth attacks [Sun, et al. (2019)]
- Man-in-the-Middle and Spoofing Attacks on Sensor Nets
  - Effects on CRLB in parameter estimation [Zhang, et al. (2018)]

Summary

- IoT requirements call for new fundamentals
- For latency: IoT requires tight latency tolerances
  - Finite blocklength IT helps assess latency in IoT applications, where the physical layer may predominate
- For security:
  - The wireless physical layer offers resources for providing some degree of security in IoT, where complexity and infrastructure constraints challenge traditional methods

Summary – Cont'd

- These are theoretical constructs - there are many needs to connect this kind of analysis to real networks, e.g.
  - interactions with higher layers (especially latency)
  - practical schemes to approach fundamental limits
- A rich area with much work left to do!


Thank You!