POWERT Channels: A Novel Class of Covert Communication Exploiting Power Management Vulnerabilities

S. Karen Khatamifard, Longfei Wang, Amitabh Das, Selcuk Kose, Ulya R. Karpuzcu

UNIVERSITY OF MINNESOTA

USF UNIVERSITY OF SOUTH FLORIDA.

UNIVERSITY of ROCHESTER

POWer

POWer + covERT

POWer + covERT = POWERT

POWer + covERT = POWERT

Generic

POWer + covERT = POWERT

Generic

No privilege needed

POWer + covERT = POWERT

Generic

No privilege needed

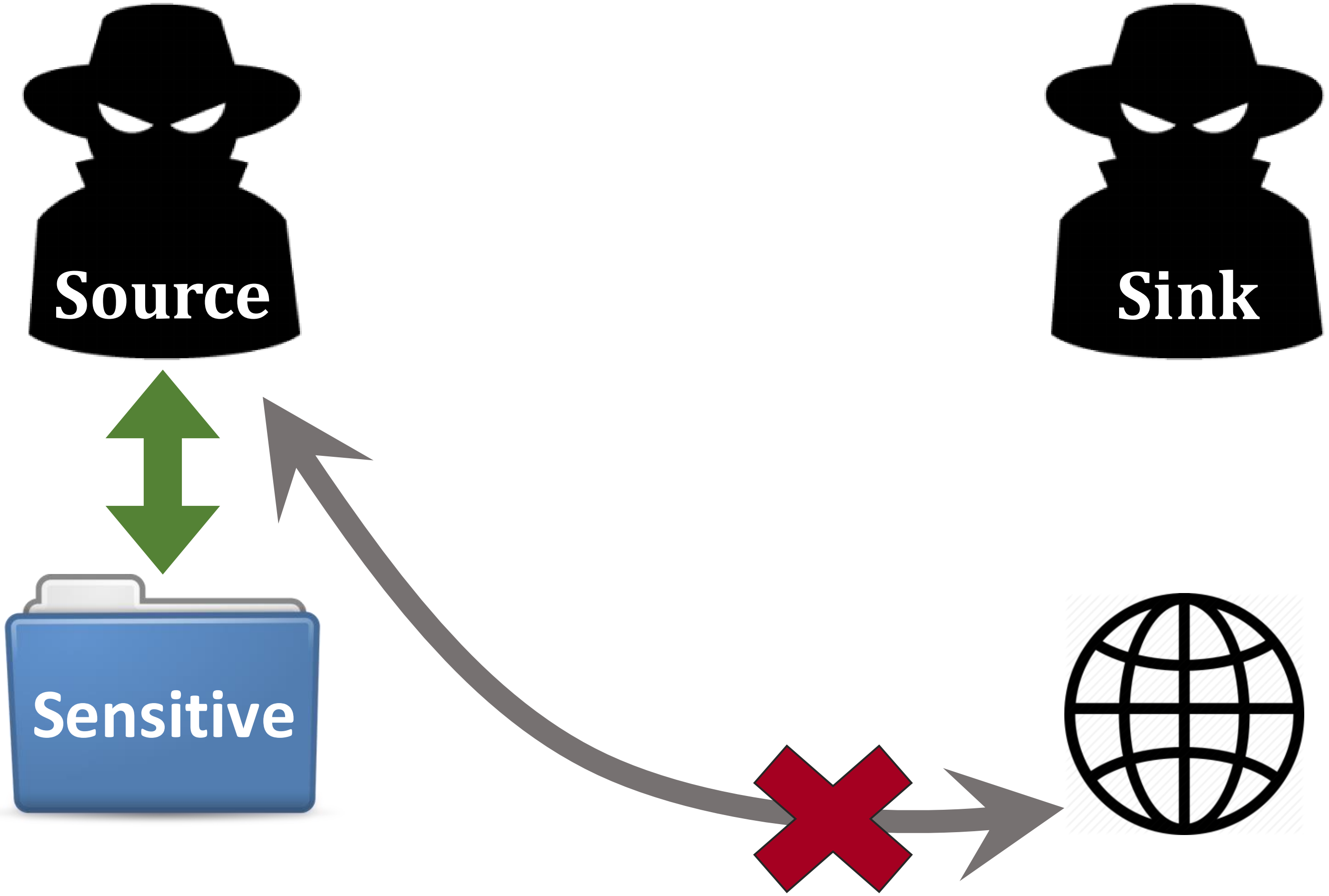
Countermeasure?

Covert Channel

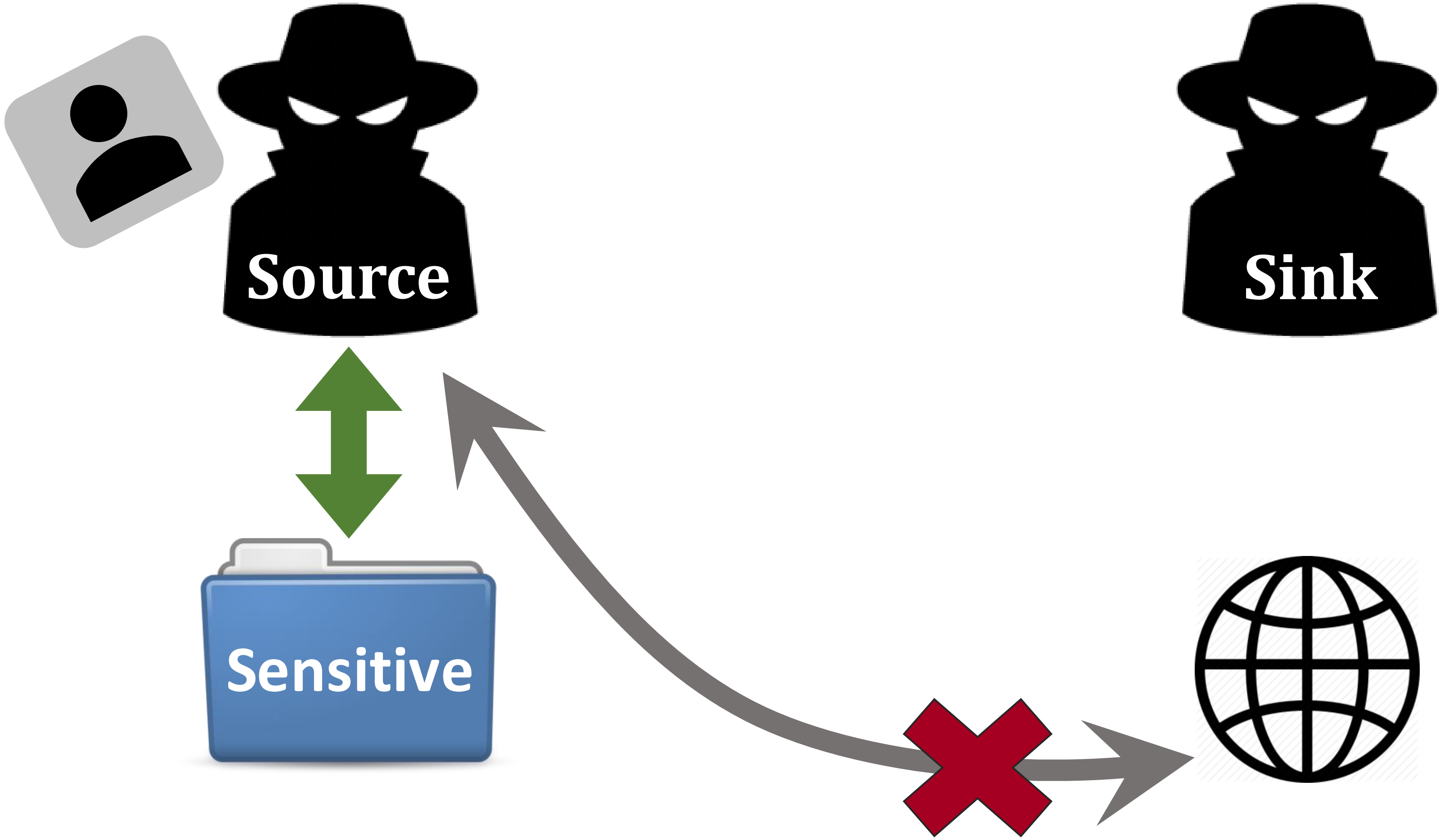
Source

Sink

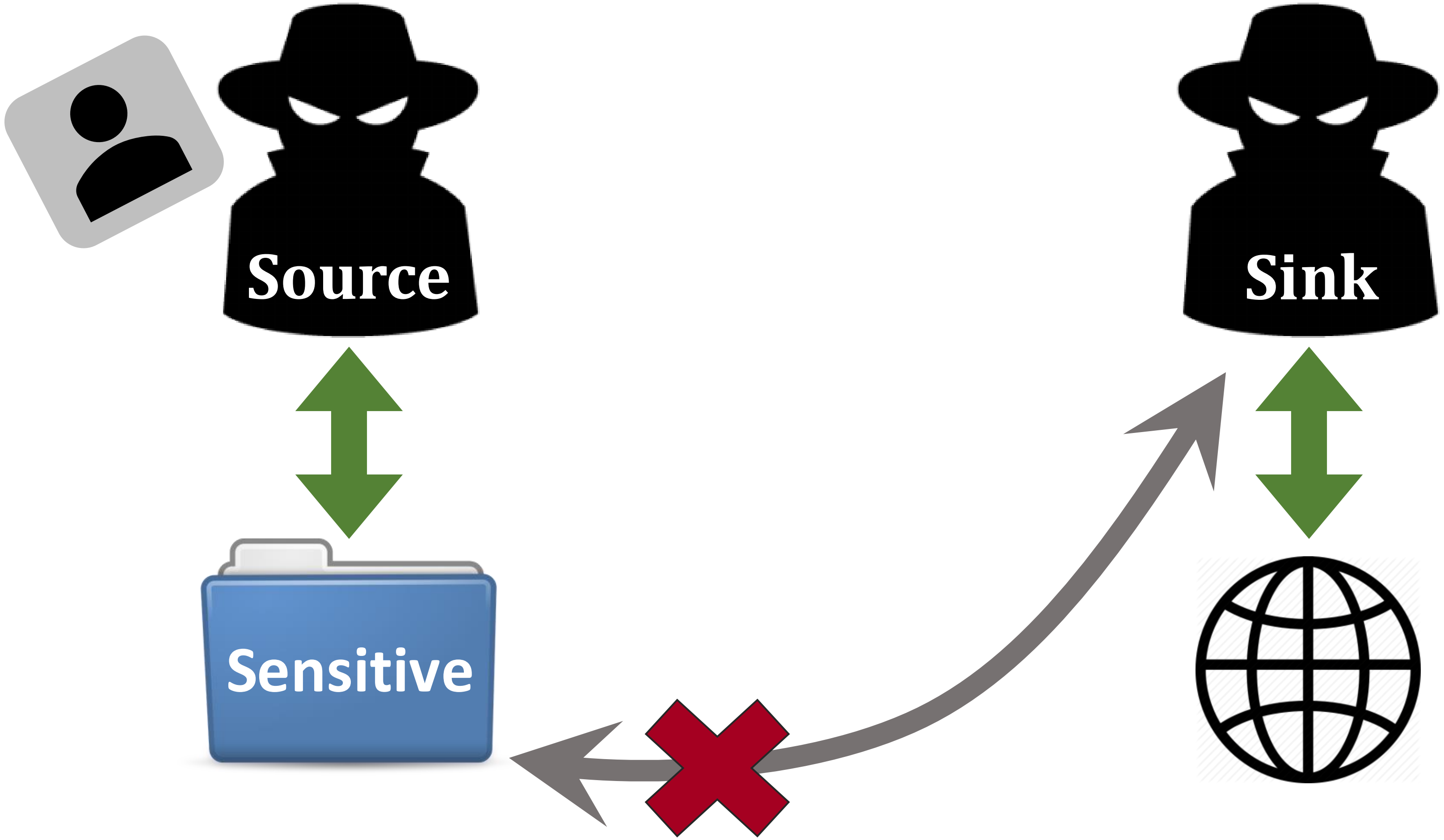
Covert Channel



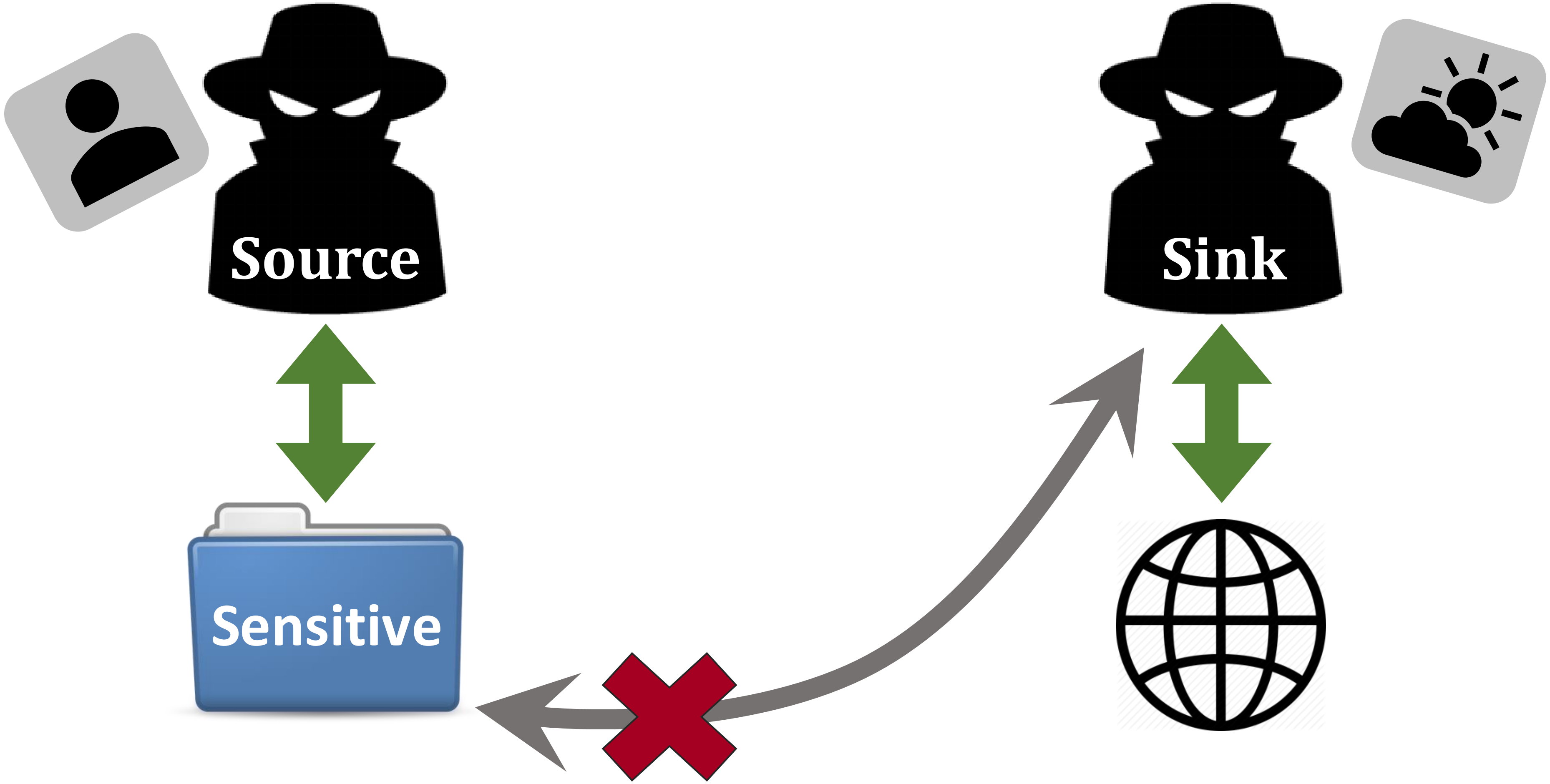
Covert Channel



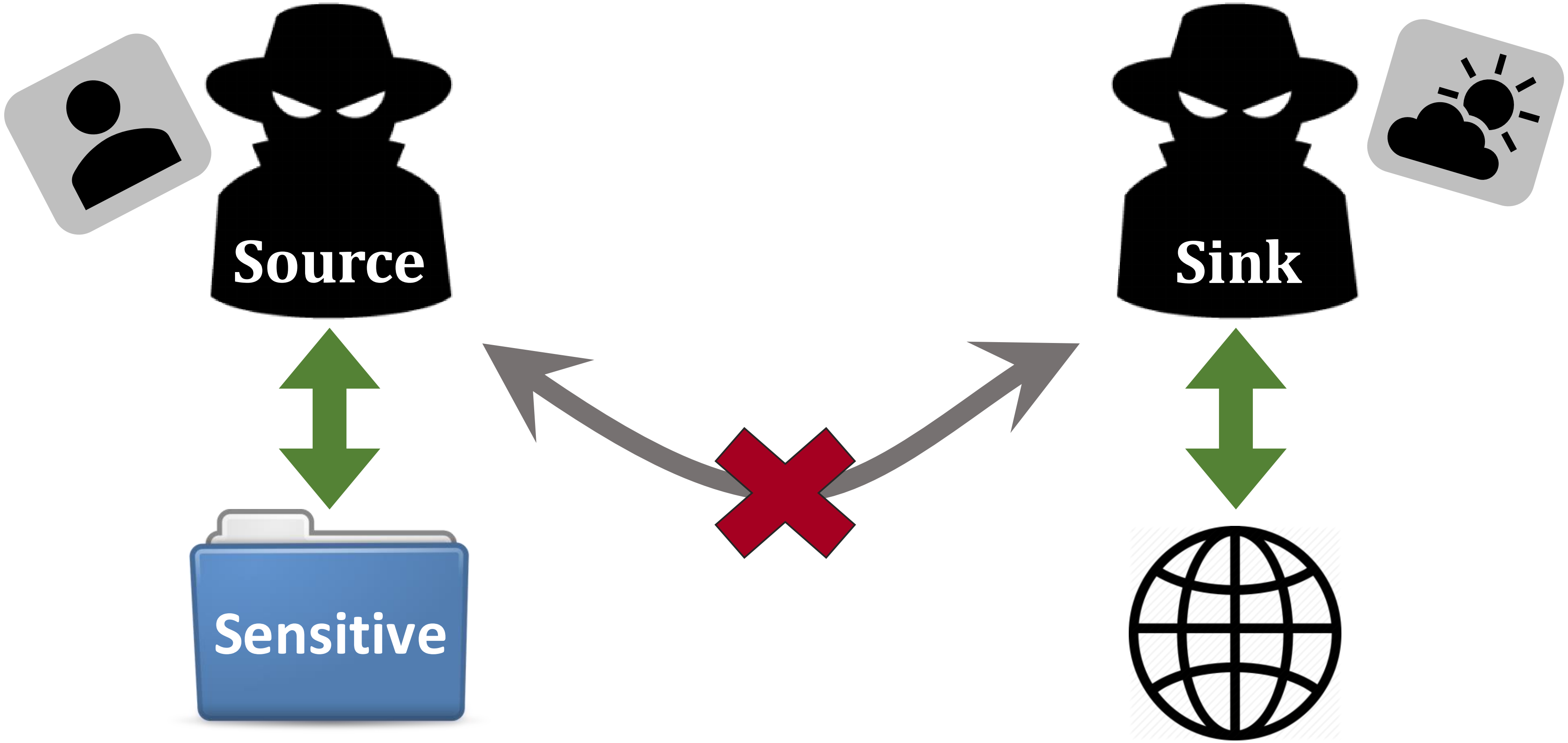
Covert Channel



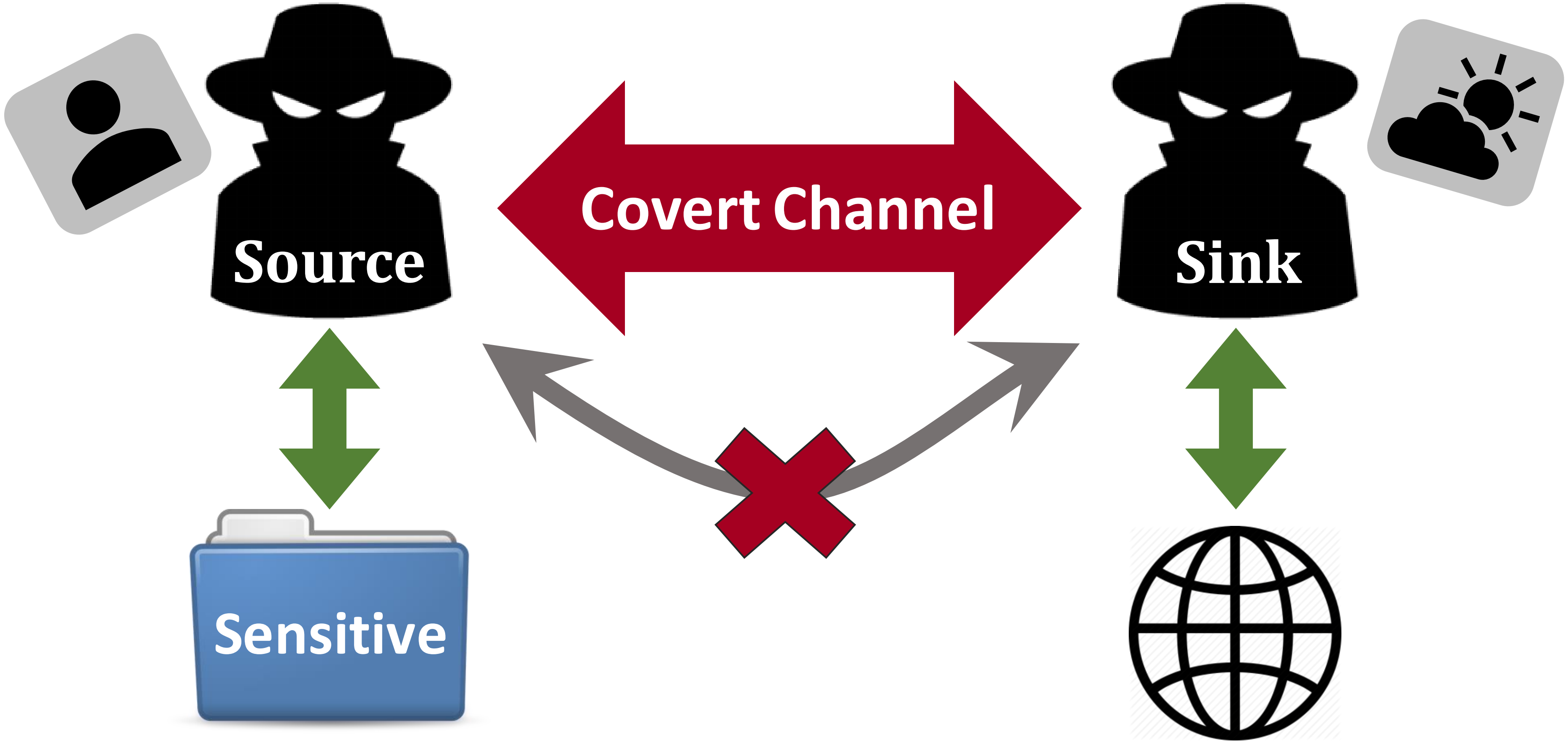
Covert Channel



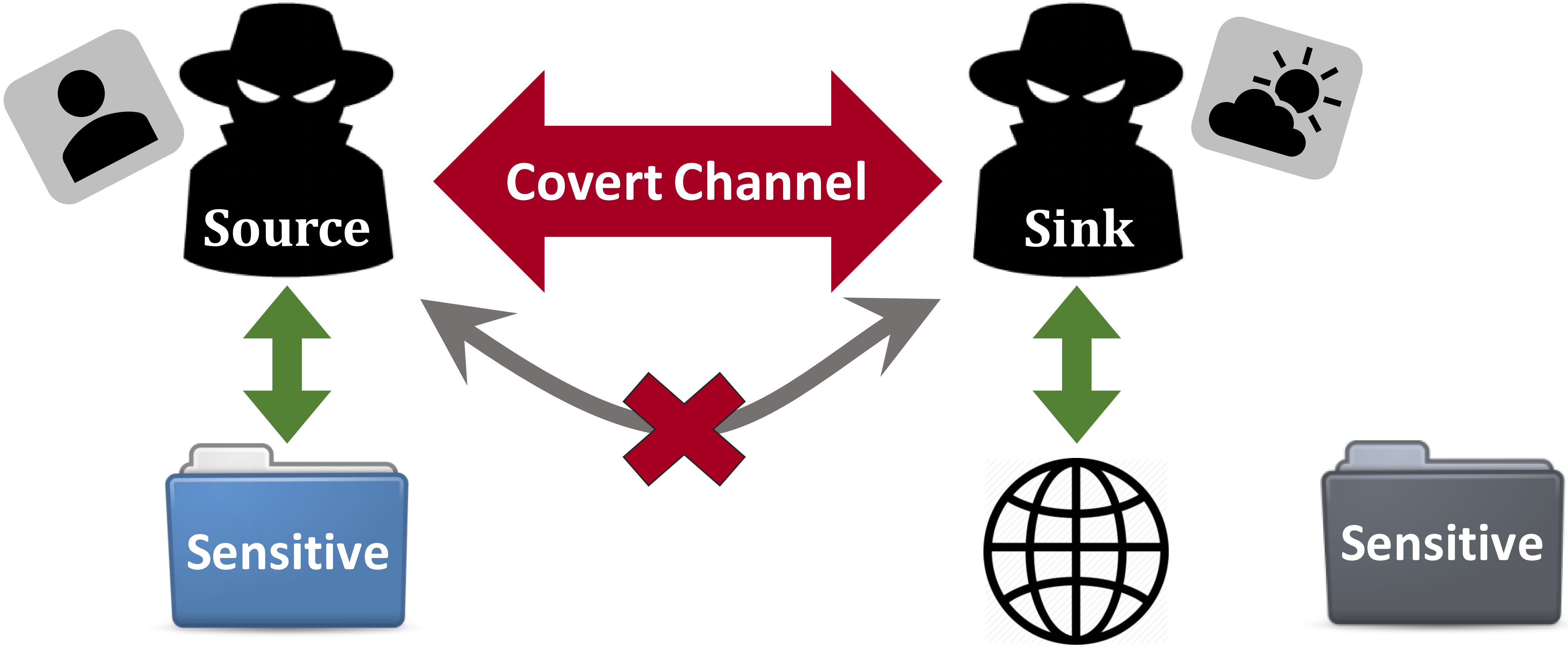
Covert Channel



Covert Channel



Covert Channel



Power Management (PM): Basics

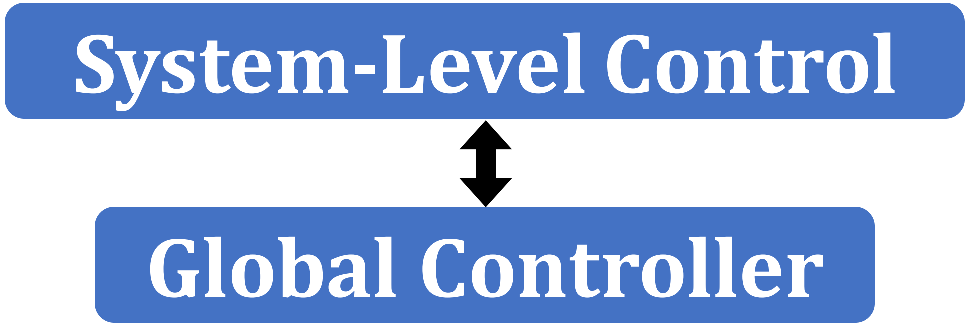
[P. Bose et. al., DATE, 2012.]

Power Management (PM): Basics

System-Level Control

[P. Bose et. al., DATE, 2012.]

Power Management (PM): Basics

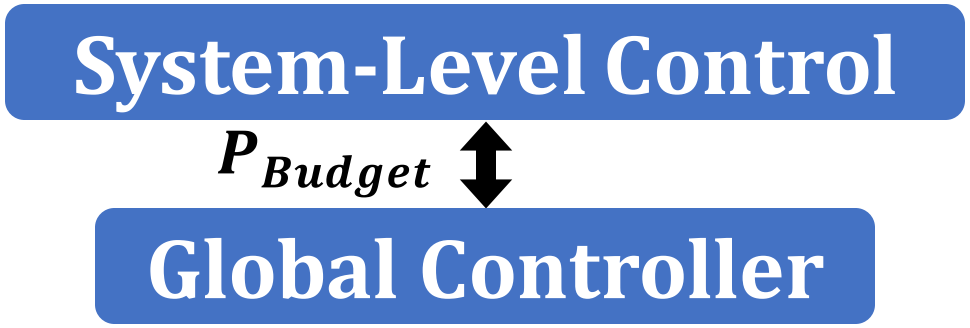


System-Level Control

Global Controller

[P. Bose et. al., DATE, 2012.]

Power Management (PM): Basics



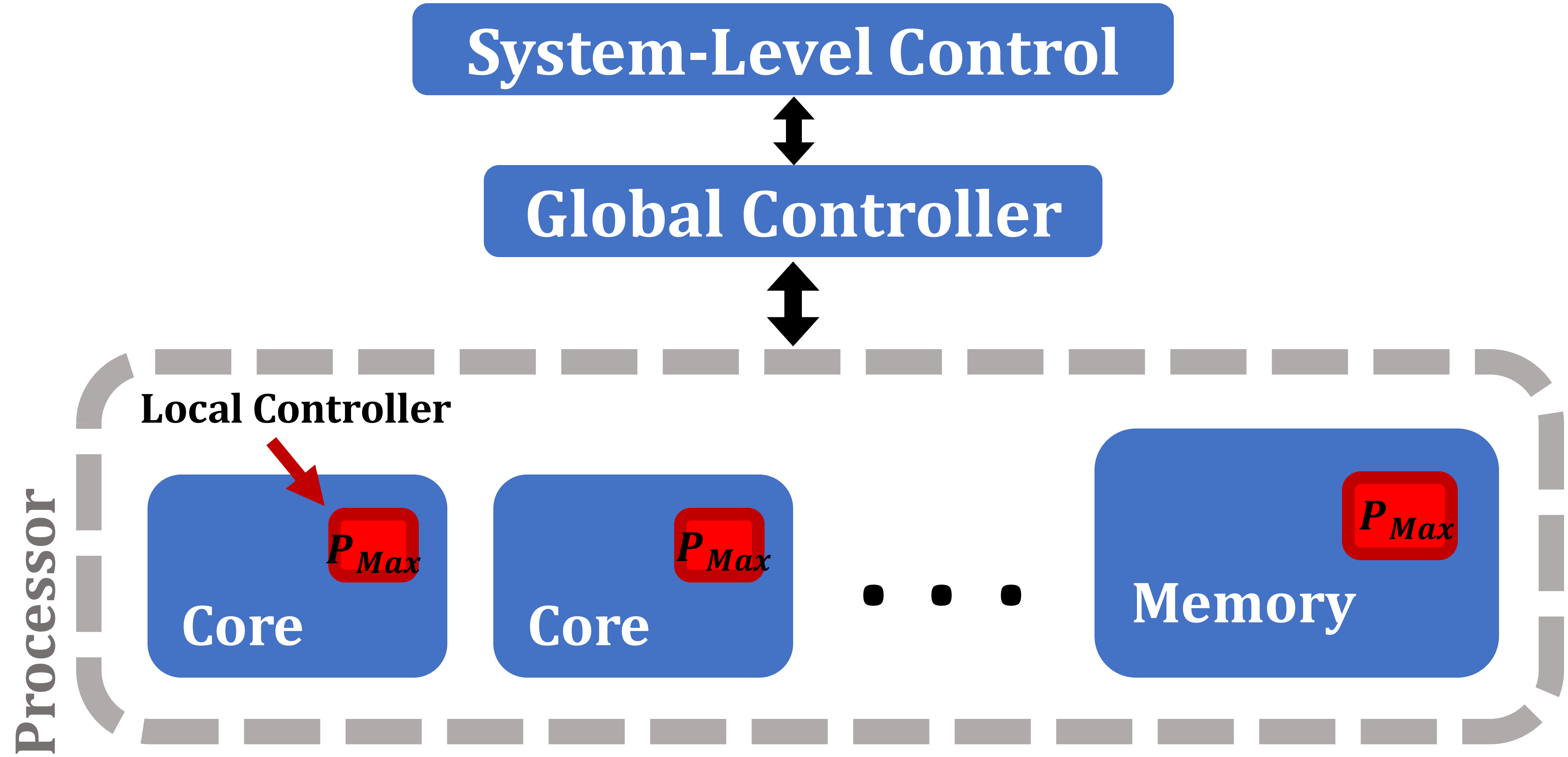
System-Level Control

P_{Budget}

Global Controller

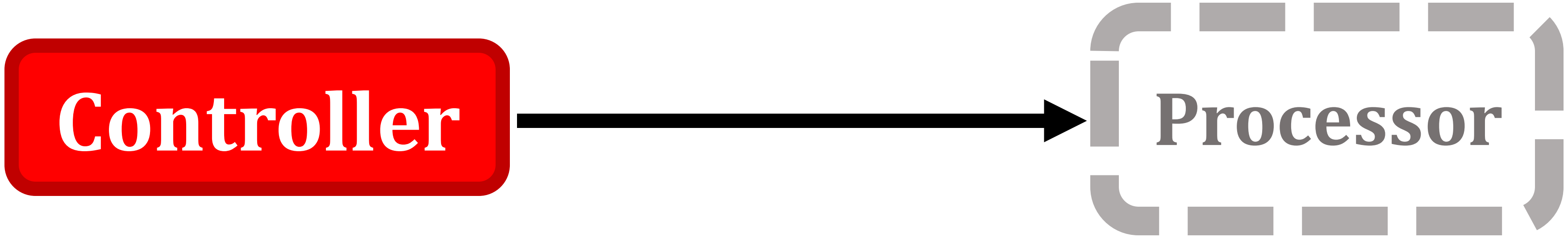
[P. Bose et. al., DATE, 2012.]

Power Management (PM): Basics



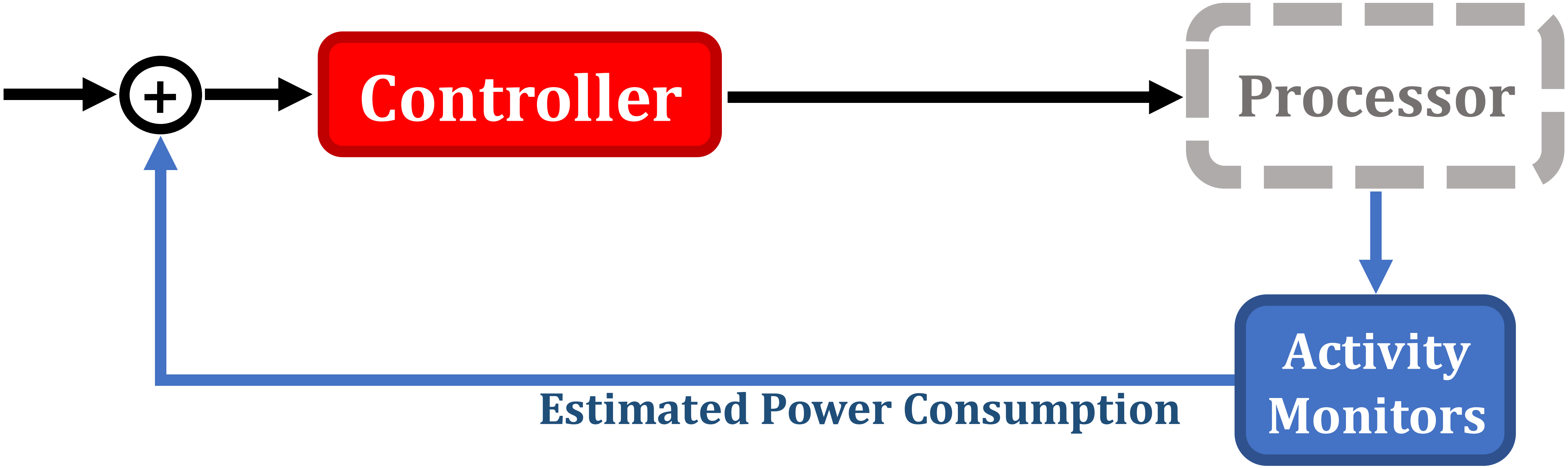
[P. Bose et. al., DATE, 2012.]

Power Management: Control Loop



[P. Bose et. al., DATE, 2012.]

Power Management: Control Loop



Controller

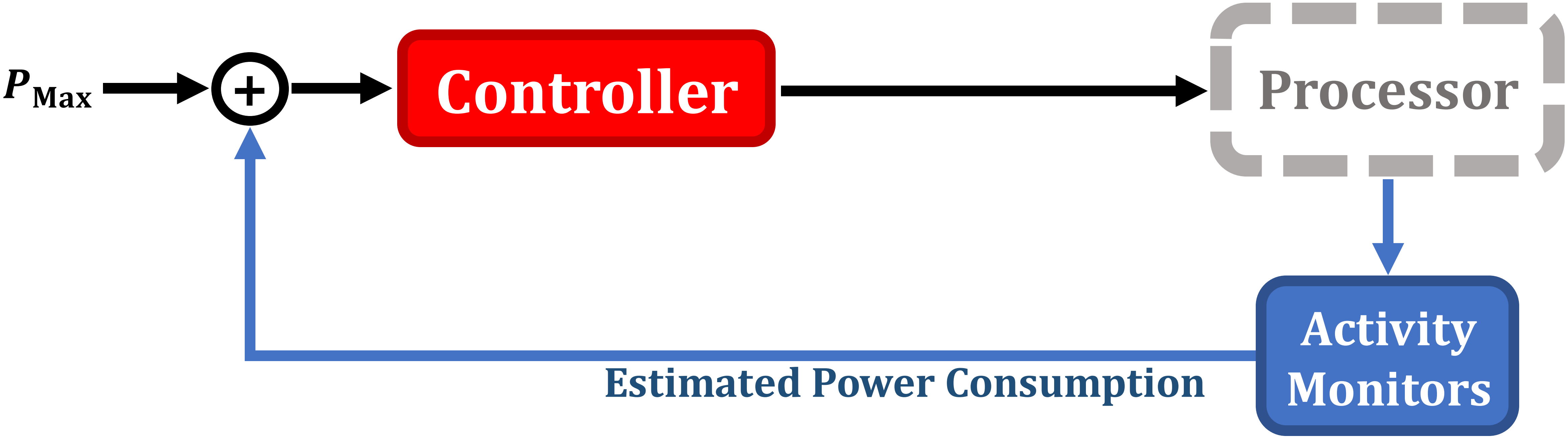
Processor

Activity Monitors

Estimated Power Consumption

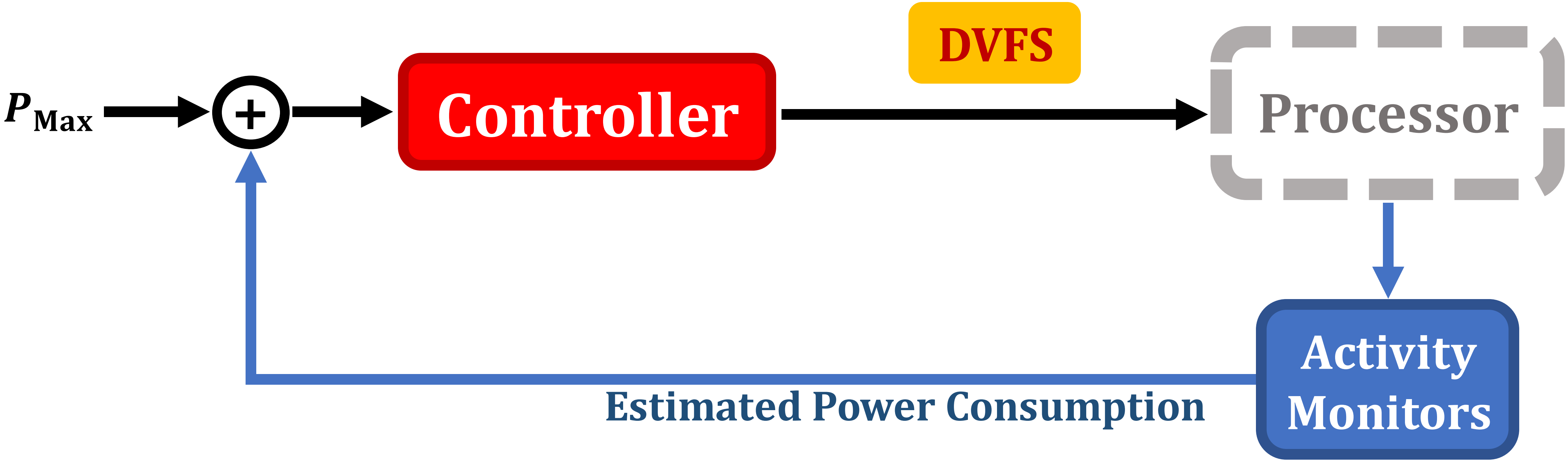
[P. Bose et. al., DATE, 2012.]

Power Management: Control Loop



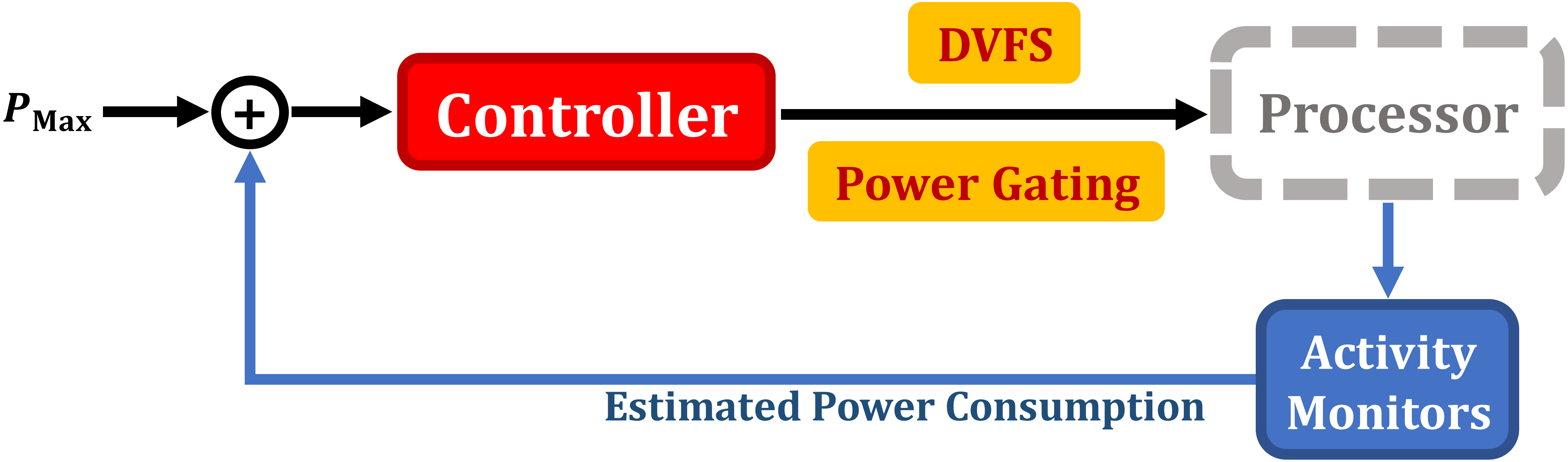
[P. Bose et. al., DATE, 2012.]

Power Management: Control Loop



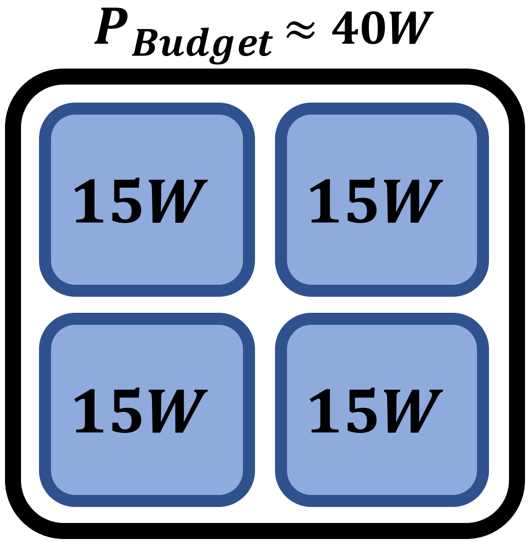
[P. Bose et. al., DATE, 2012.]

Power Management: Control Loop



[P. Bose et. al., DATE, 2012.]

Power Management: An Example



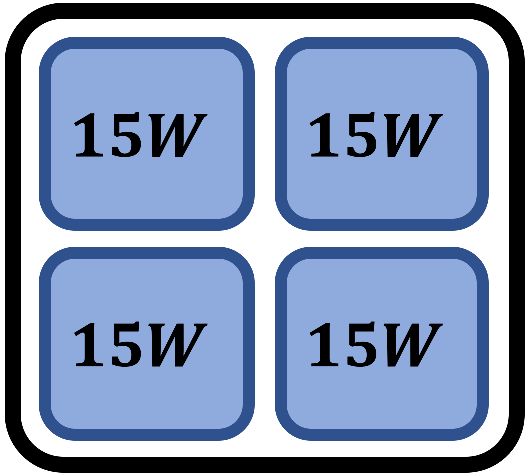
$P_{Budget} \approx 40W$

$15W$ $15W$

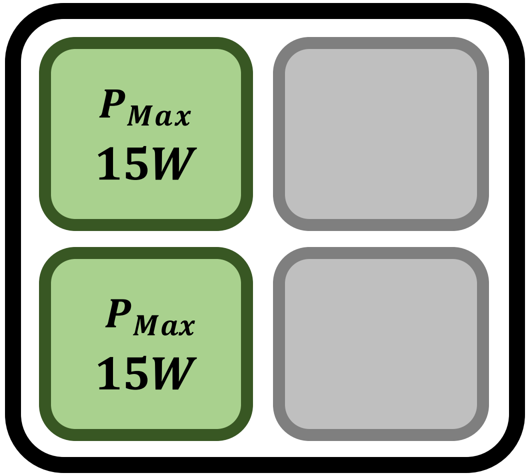
$15W$ $15W$

Power Management: An Example

$P_{Budget} \approx 40W$



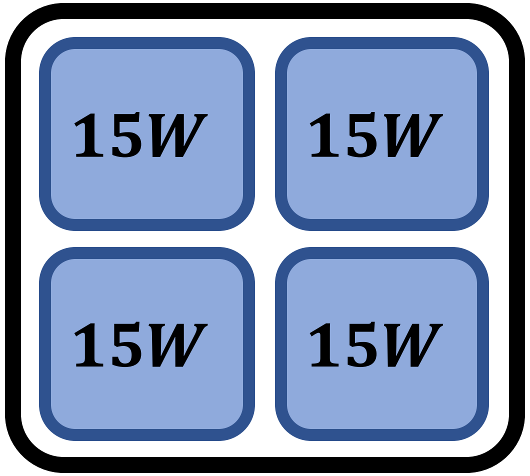
$P_{Budget} \approx 40W$



2 active cores

Power Management: An Example

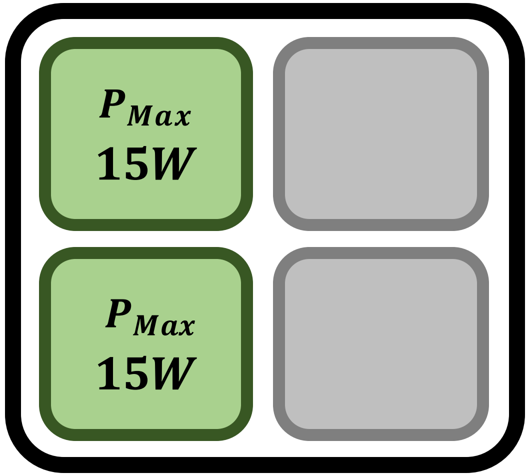
$P_{Budget} \approx 40W$



$15W$ $15W$

$15W$ $15W$

$P_{Budget} \approx 40W$

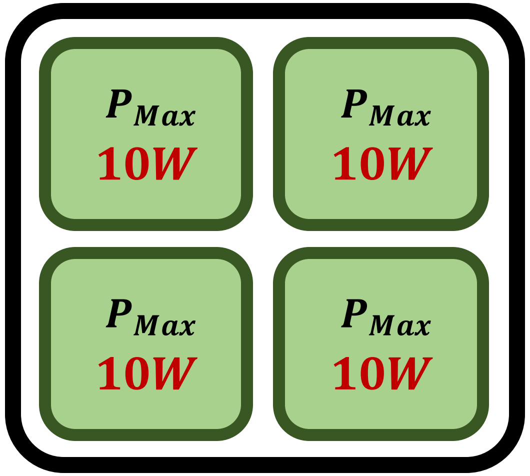


P_{Max} $15W$

P_{Max} $15W$

2 active cores

$P_{Budget} \approx 40W$

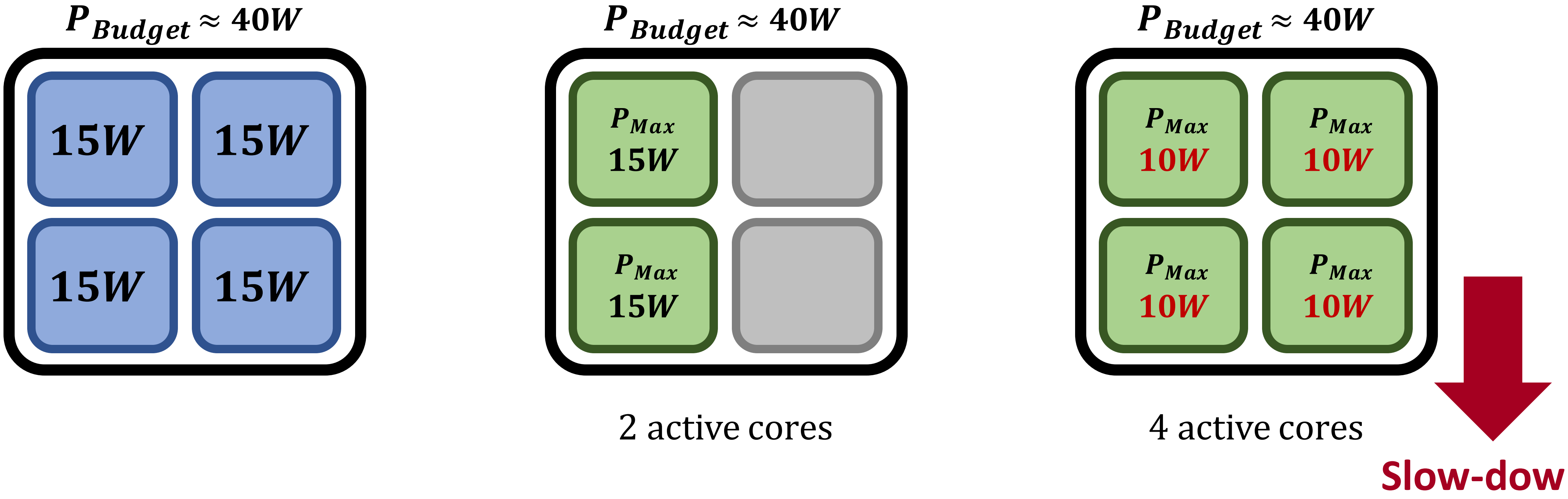


P_{Max} $10W$ P_{Max} $10W$

P_{Max} $10W$ P_{Max} $10W$

4 active cores

Power Management: An Example



$P_{Budget} \approx 40W$

$15W$ $15W$

$15W$ $15W$

$P_{Budget} \approx 40W$

P_{Max} $15W$

P_{Max} $15W$

2 active cores

$P_{Budget} \approx 40W$

P_{Max} $10W$ P_{Max} $10W$

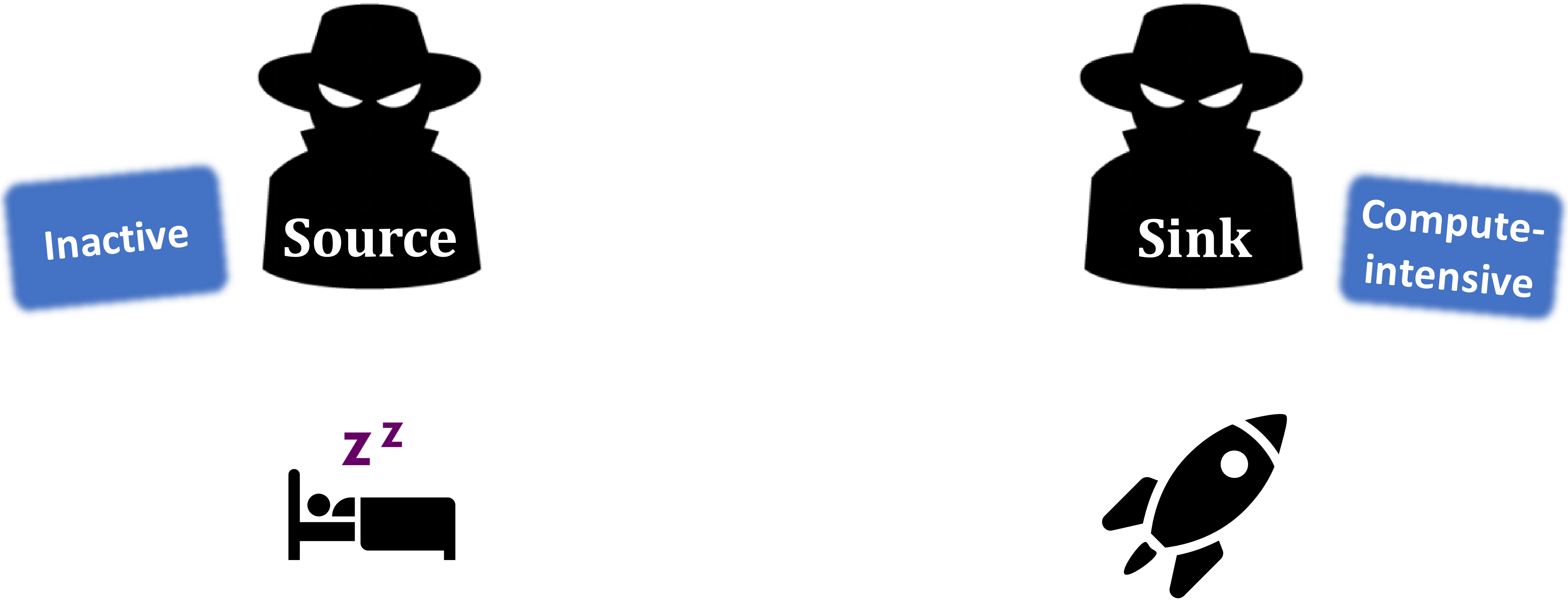
P_{Max} $10W$ P_{Max} $10W$

4 active cores

Slow-down!

Power Headroom Modulation

Power Headroom Modulation



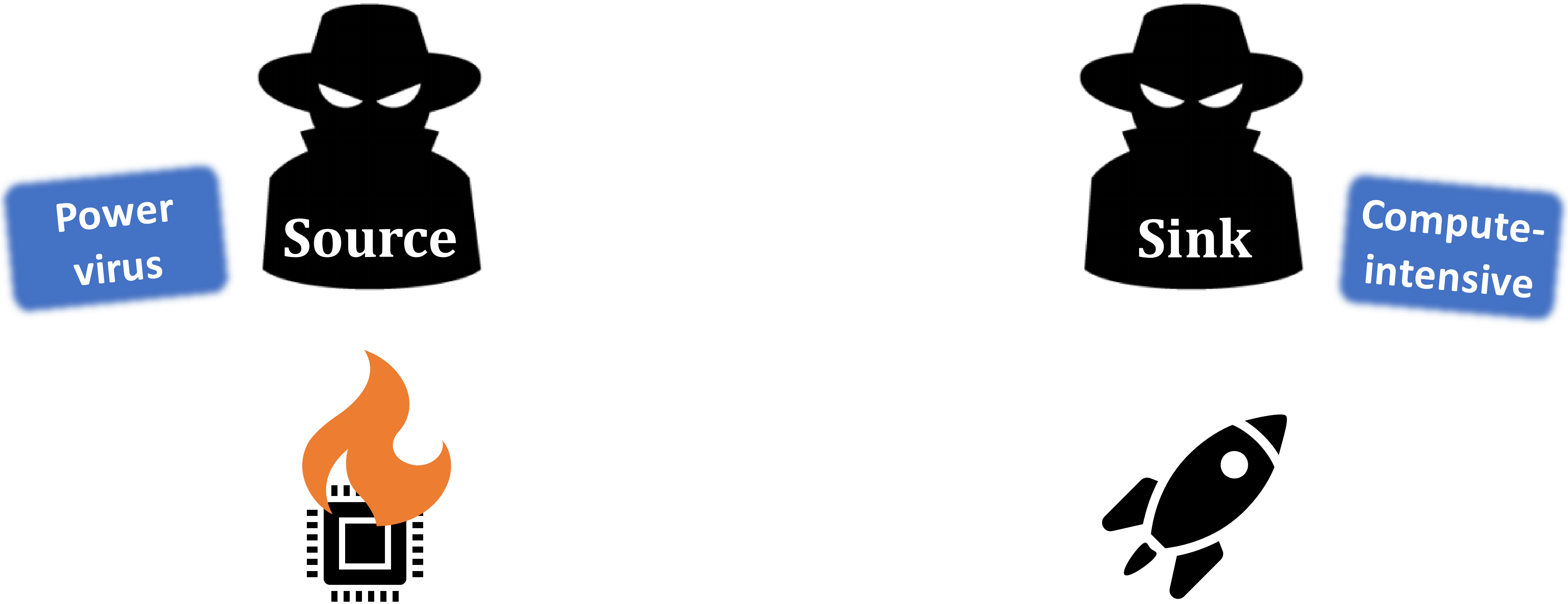
Inactive

Source

Sink

Compute-intensive

Power Headroom Modulation



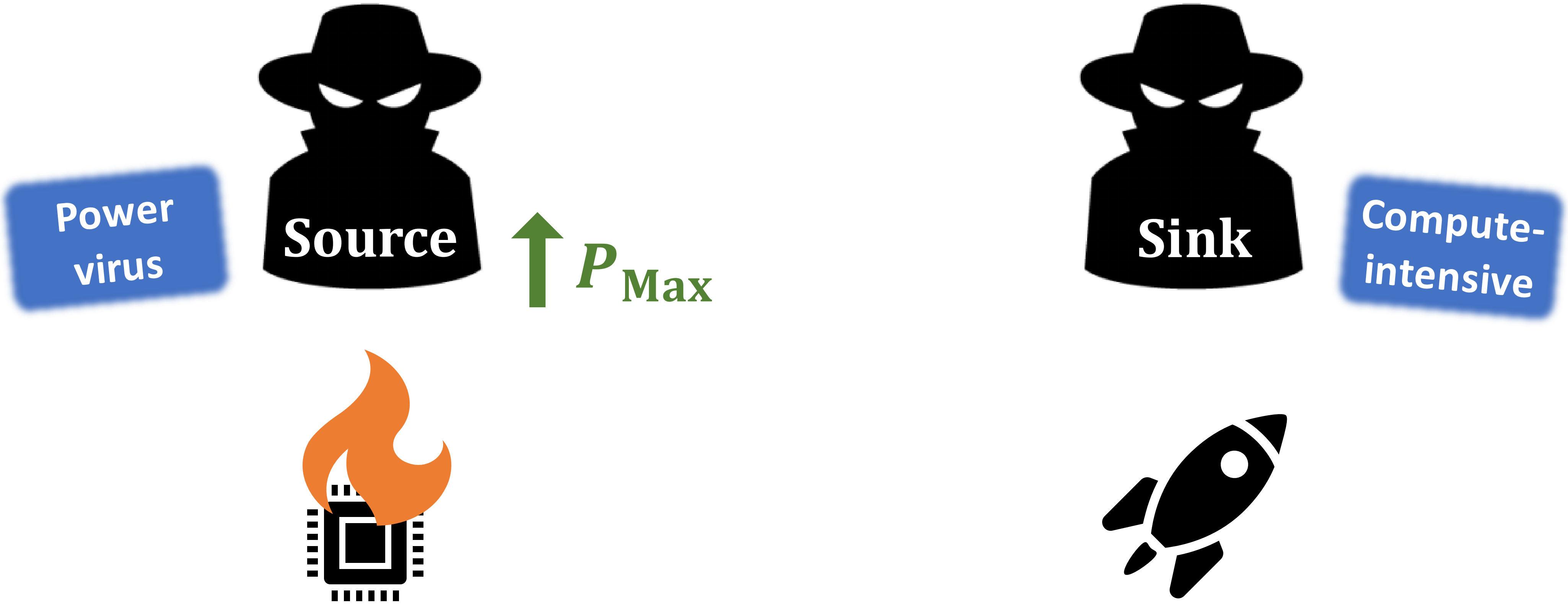
Power virus

Source

Sink

Compute-intensive

Power Headroom Modulation



Power virus

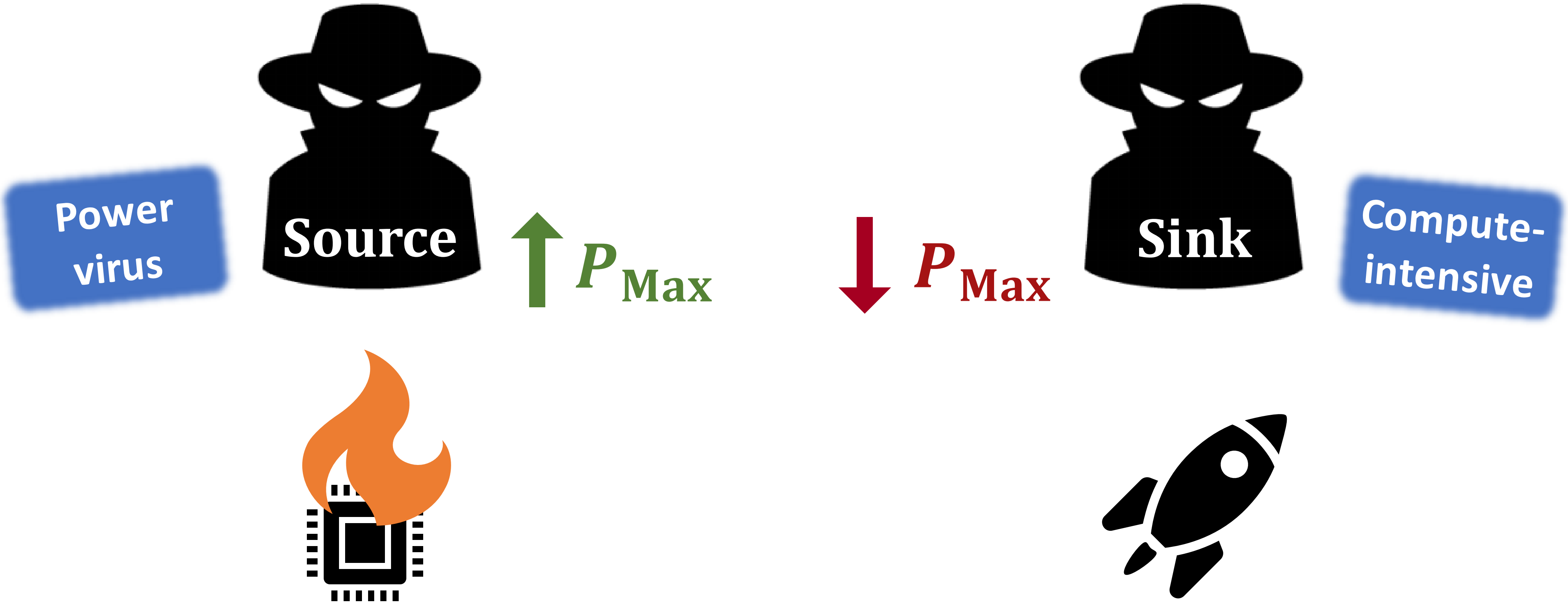
Source

↑ P_{Max}

Sink

Compute-intensive

Power Headroom Modulation



Power virus

Source

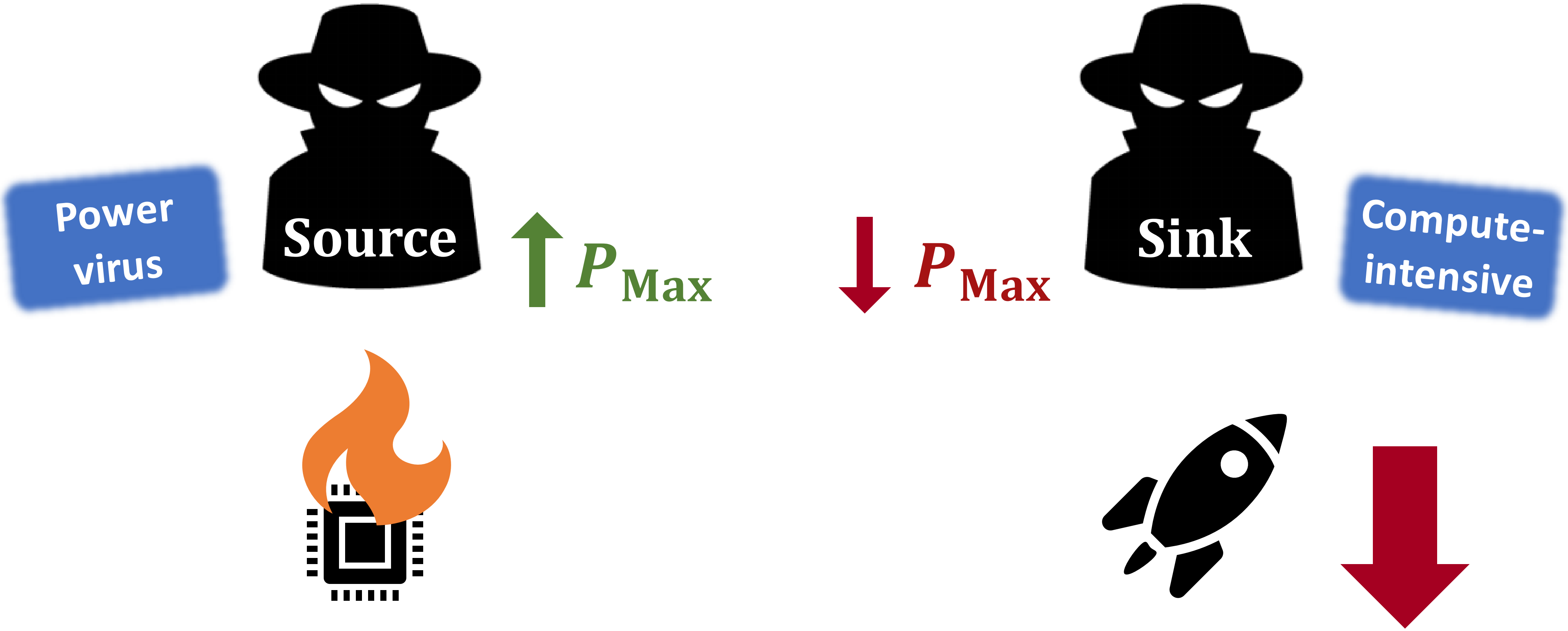
↑ P_{Max}

↓ P_{Max}

Sink

Compute-intensive

Power Headroom Modulation



Power virus

Source

↑ P_{Max}

↓ P_{Max}

Sink

Compute-intensive

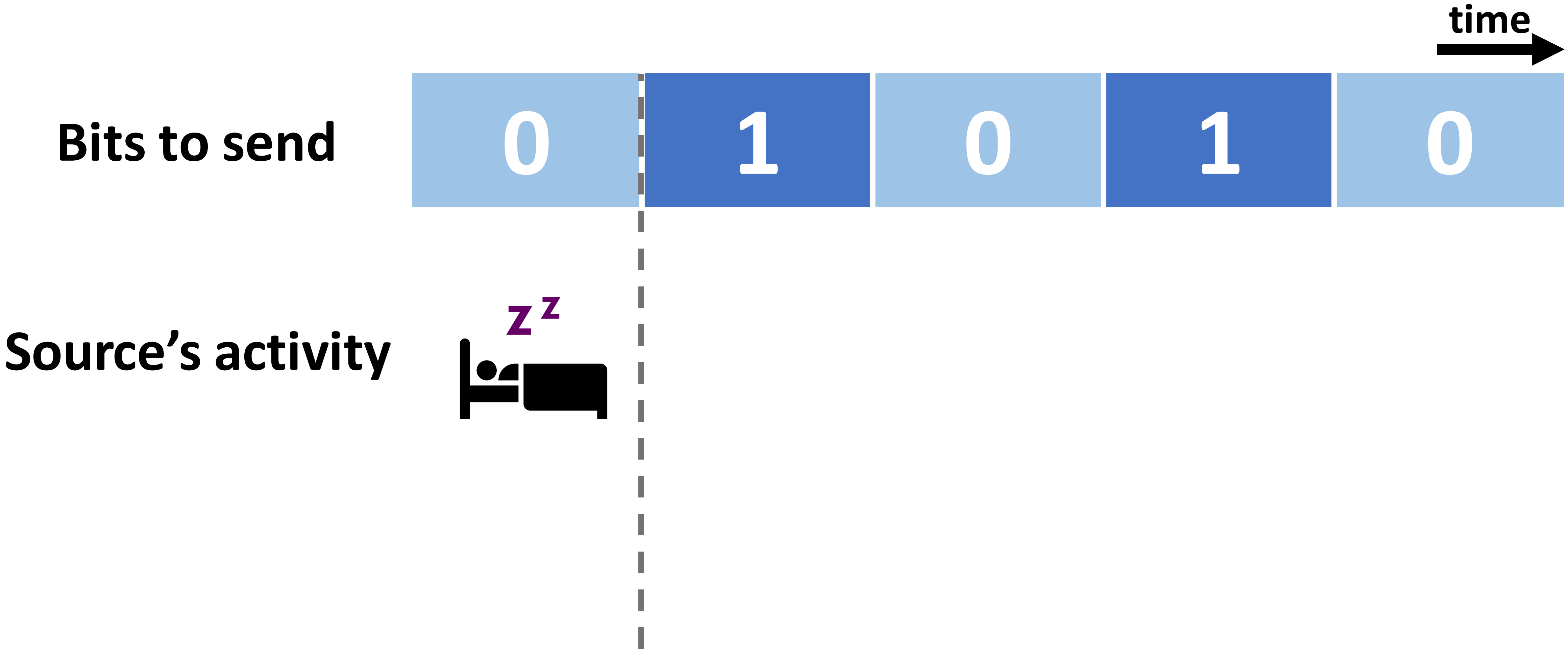
Slow-down!

Single-bit Encoding

time →

Bits to send	0	1	0	1	0

Single-bit Encoding



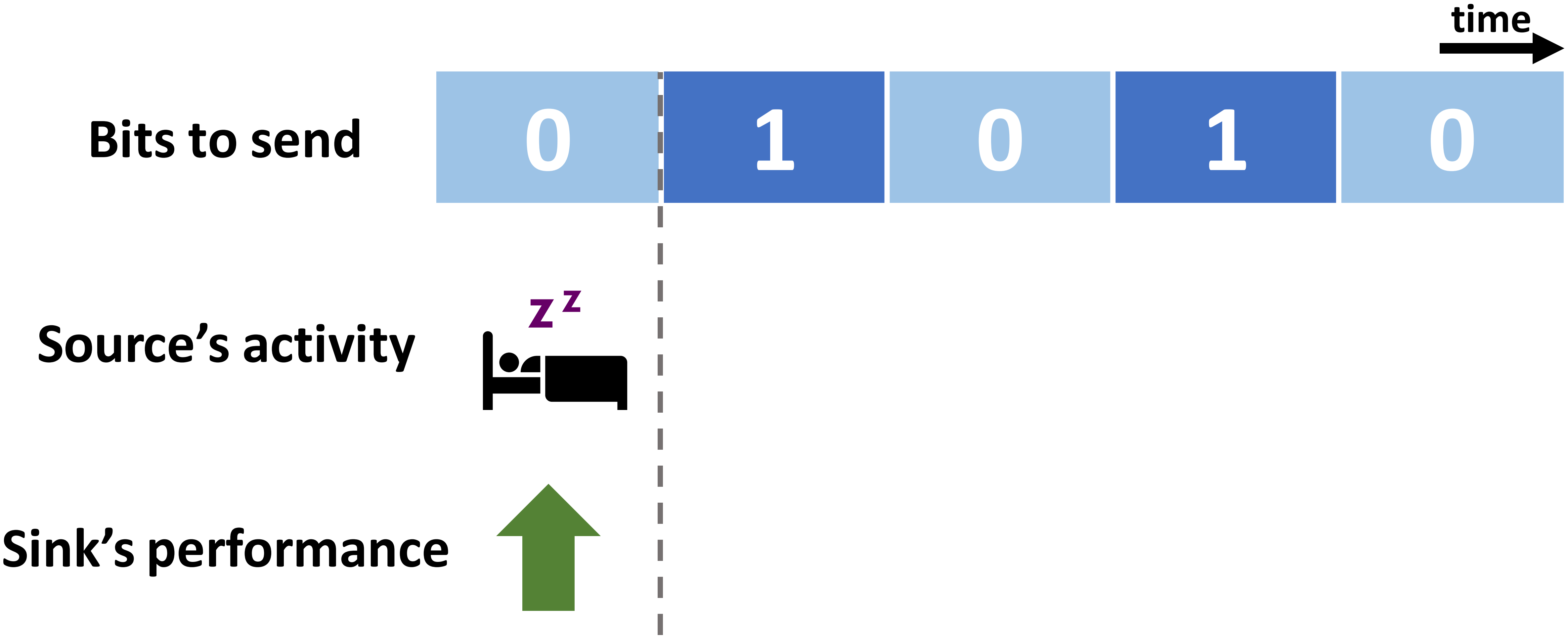
time

Bits to send

0 1 0 1 0

Source's activity

Single-bit Encoding



time

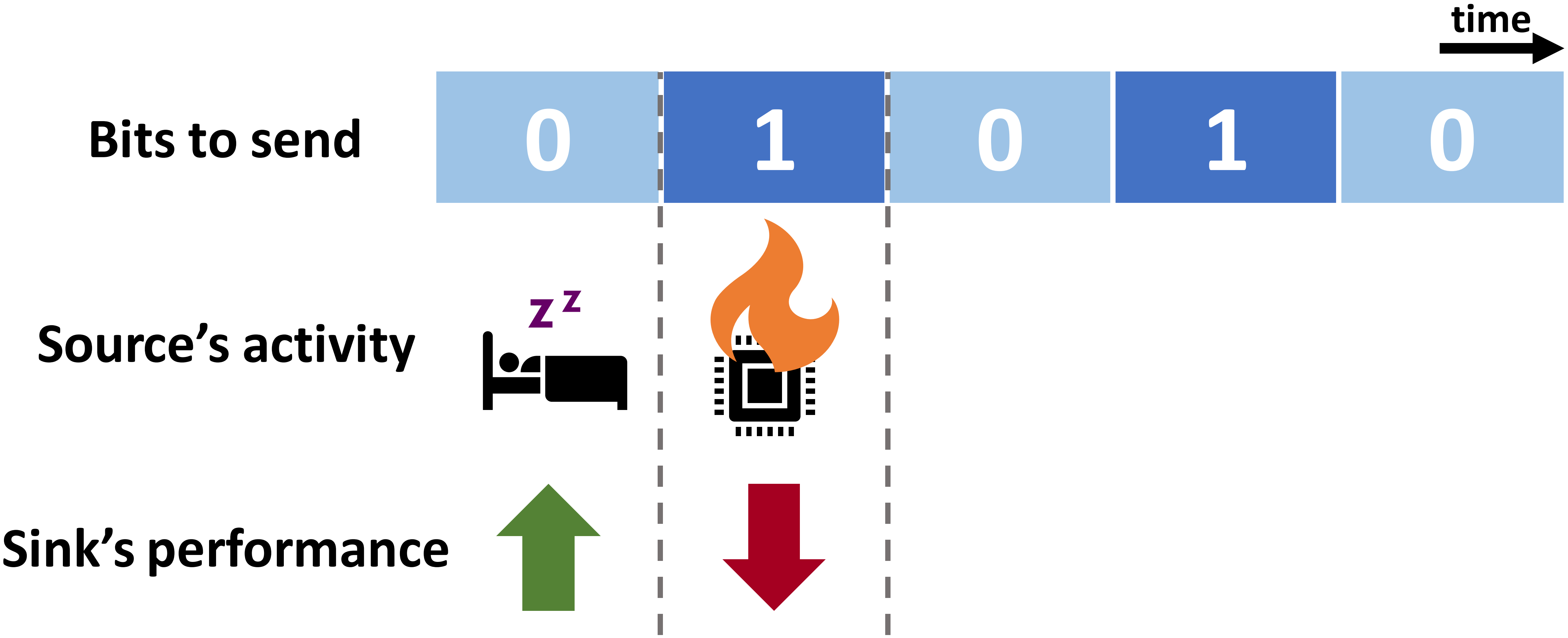
Bits to send

0	1	0	1	0

Source's activity

Sink's performance

Single-bit Encoding



time

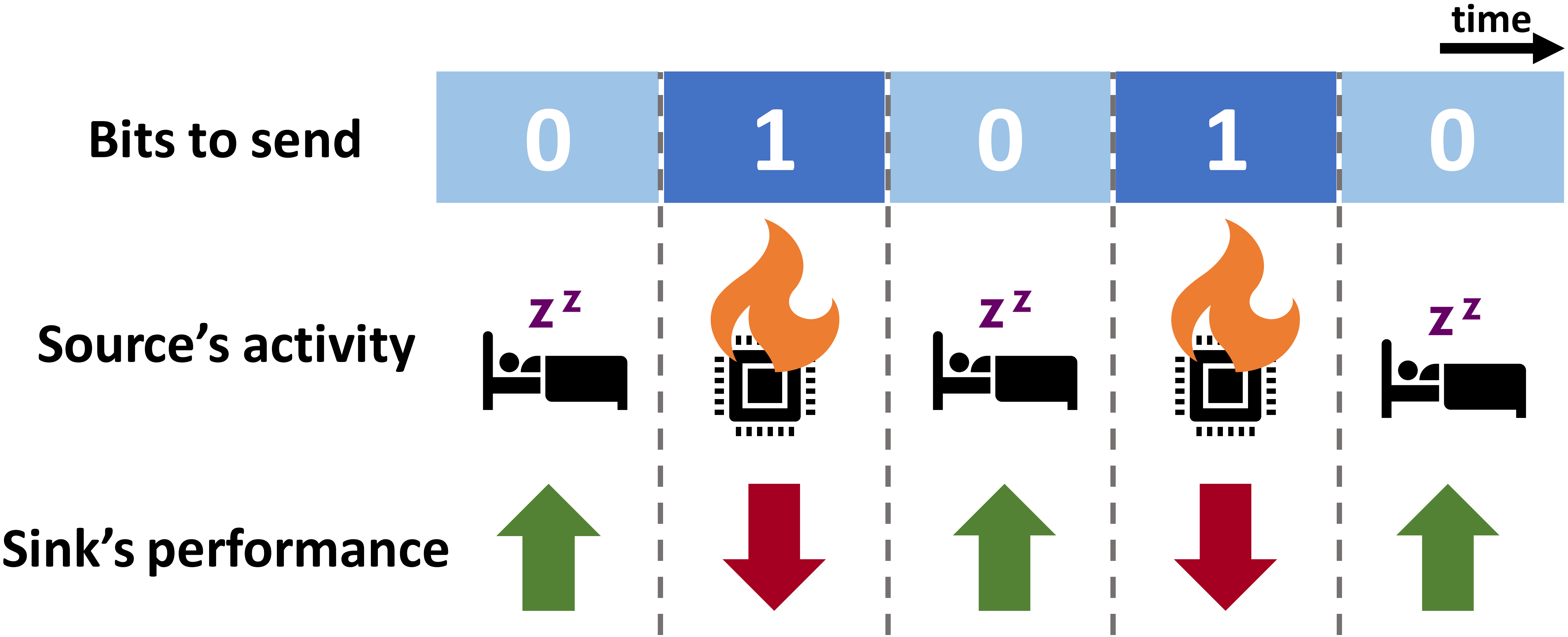
Bits to send

0	1	0	1	0

Source's activity

Sink's performance

Single-bit Encoding



time

Bits to send

0 1 0 1 0

Source’s activity

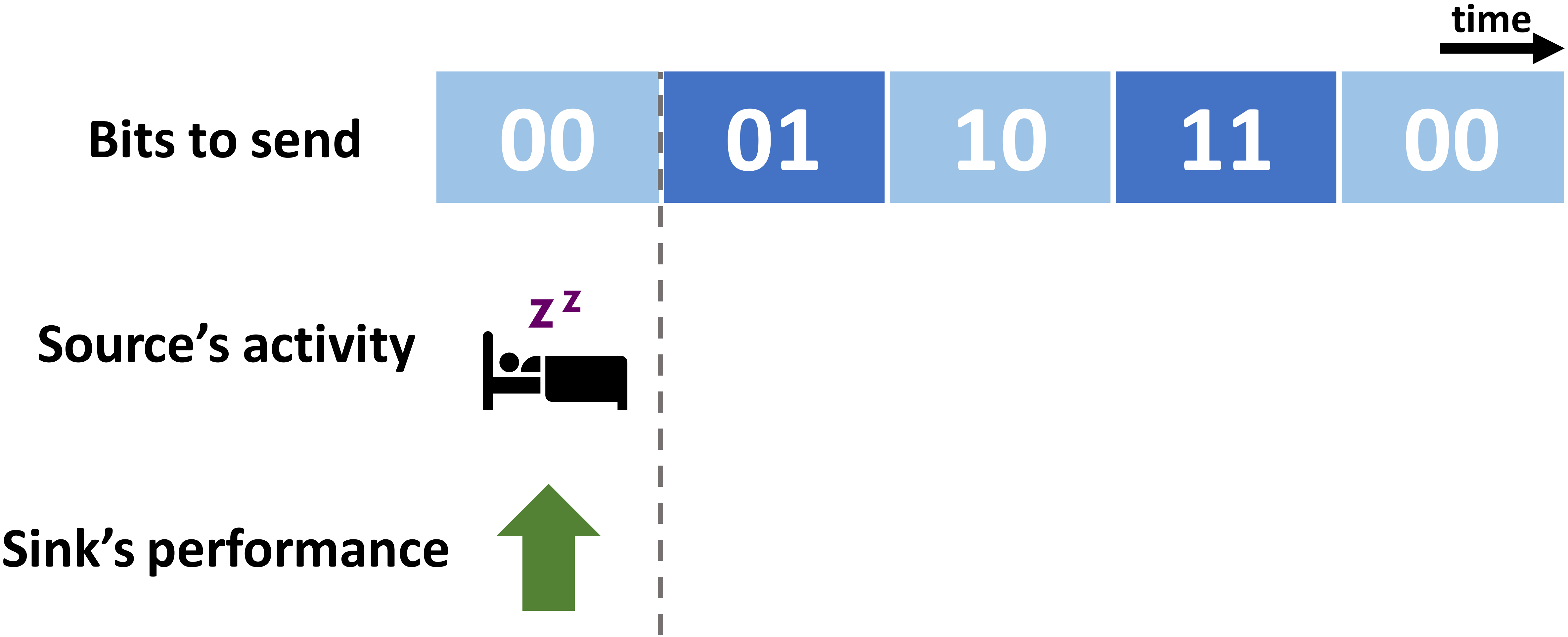
Sink’s performance

Multi-bit Encoding

time →

Bits to send	00	01	10	11	00

Multi-bit Encoding



time

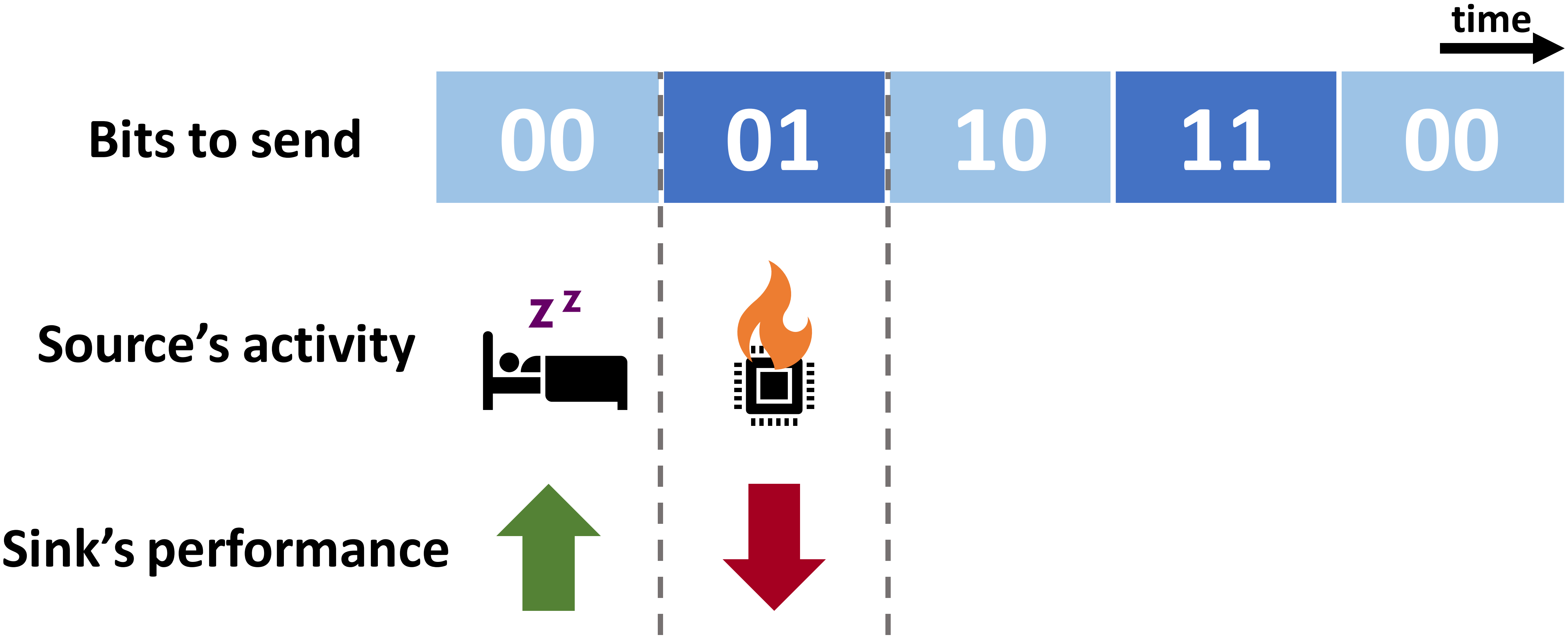
Bits to send

00 01 10 11 00

Source’s activity

Sink’s performance

Multi-bit Encoding



time

Bits to send

00

01

10

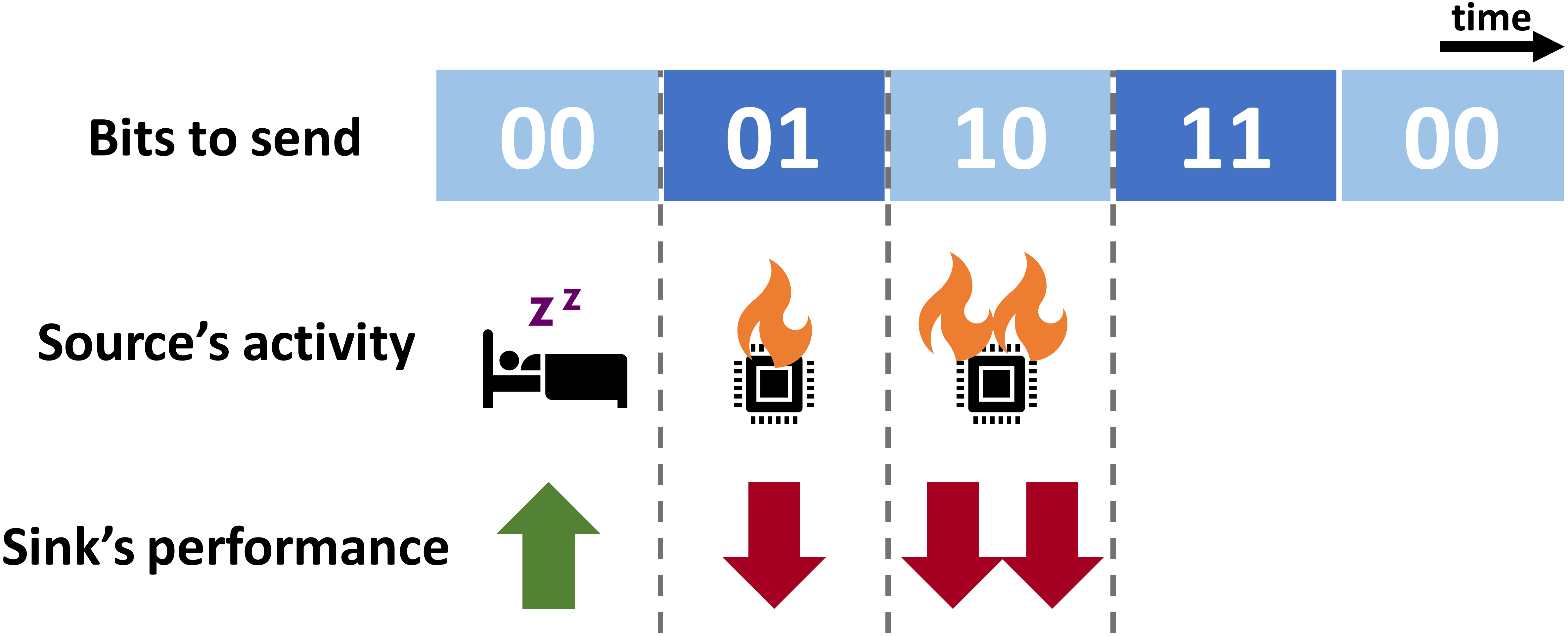
11

00

Source’s activity

Sink’s performance

Multi-bit Encoding



time

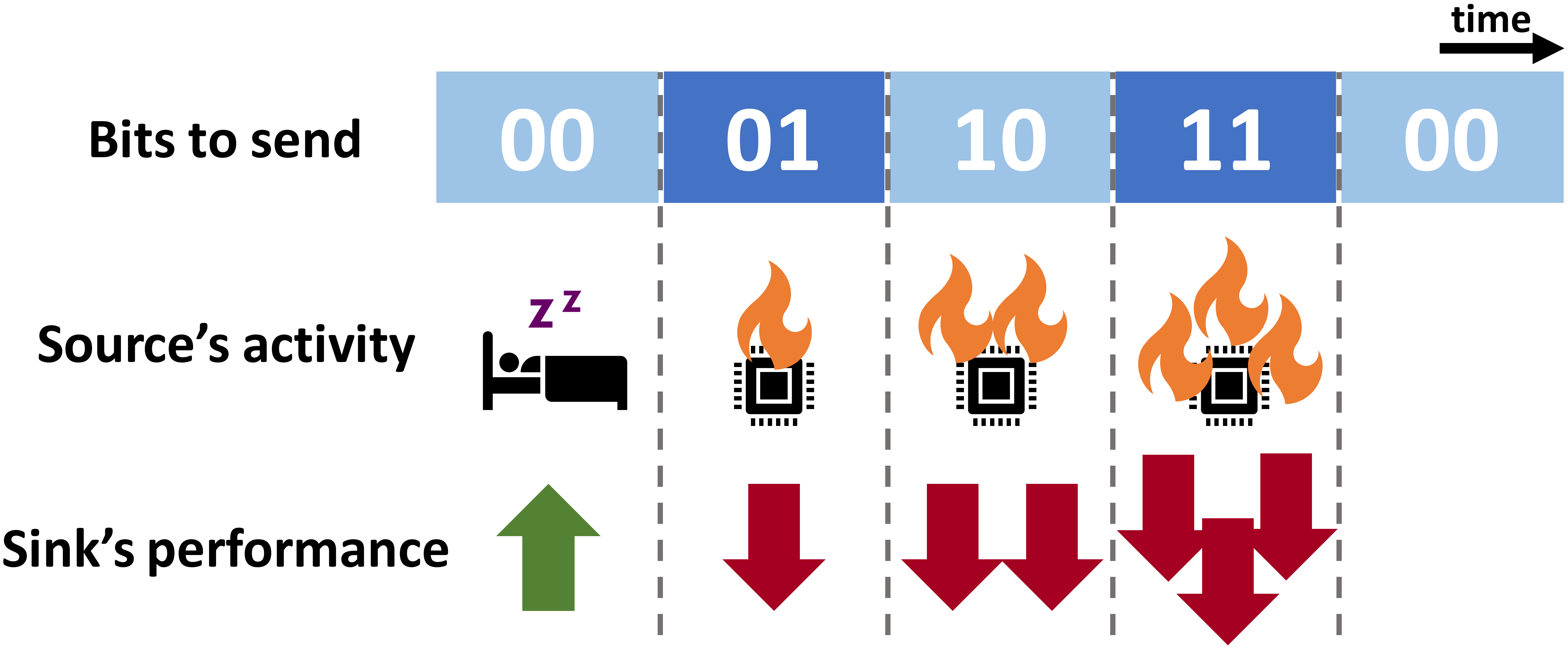
Bits to send

00 | 01 | 10 | 11 | 00

Source’s activity

Sink’s performance

Multi-bit Encoding



time

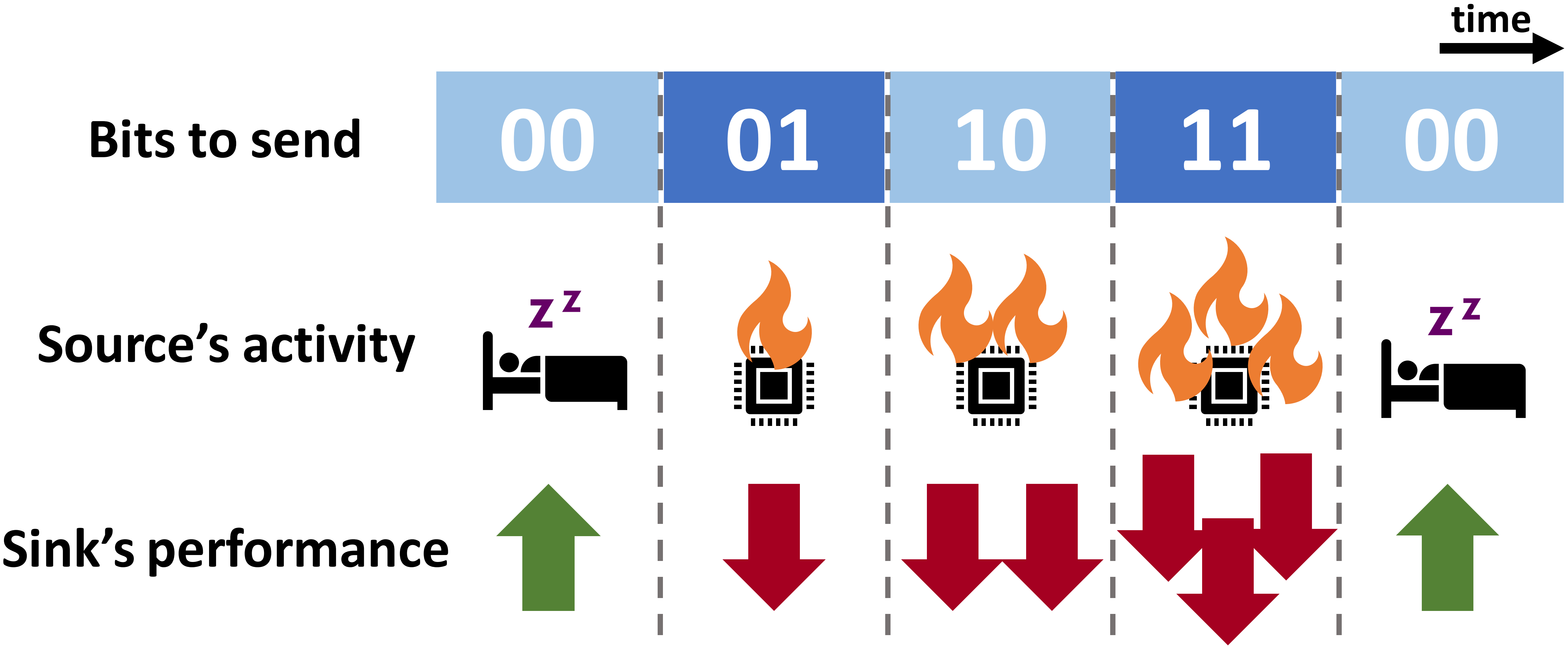
Bits to send

00	01	10	11	00

Source's activity

Sink's performance

Multi-bit Encoding



time

Bits to send

00

01

10

11

00

Source's activity

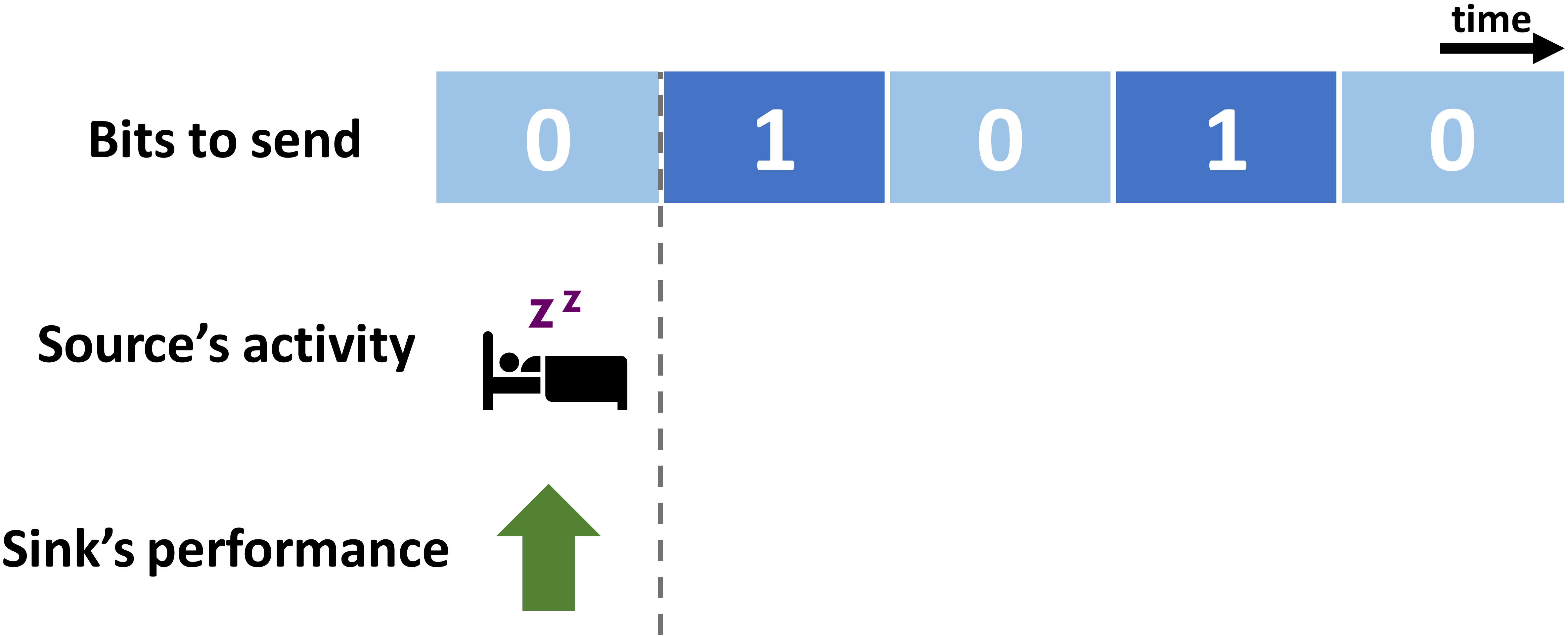
Sink's performance

Stronger Single-bit Encoding

time →

Bits to send	0	1	0	1	0

Stronger Single-bit Encoding



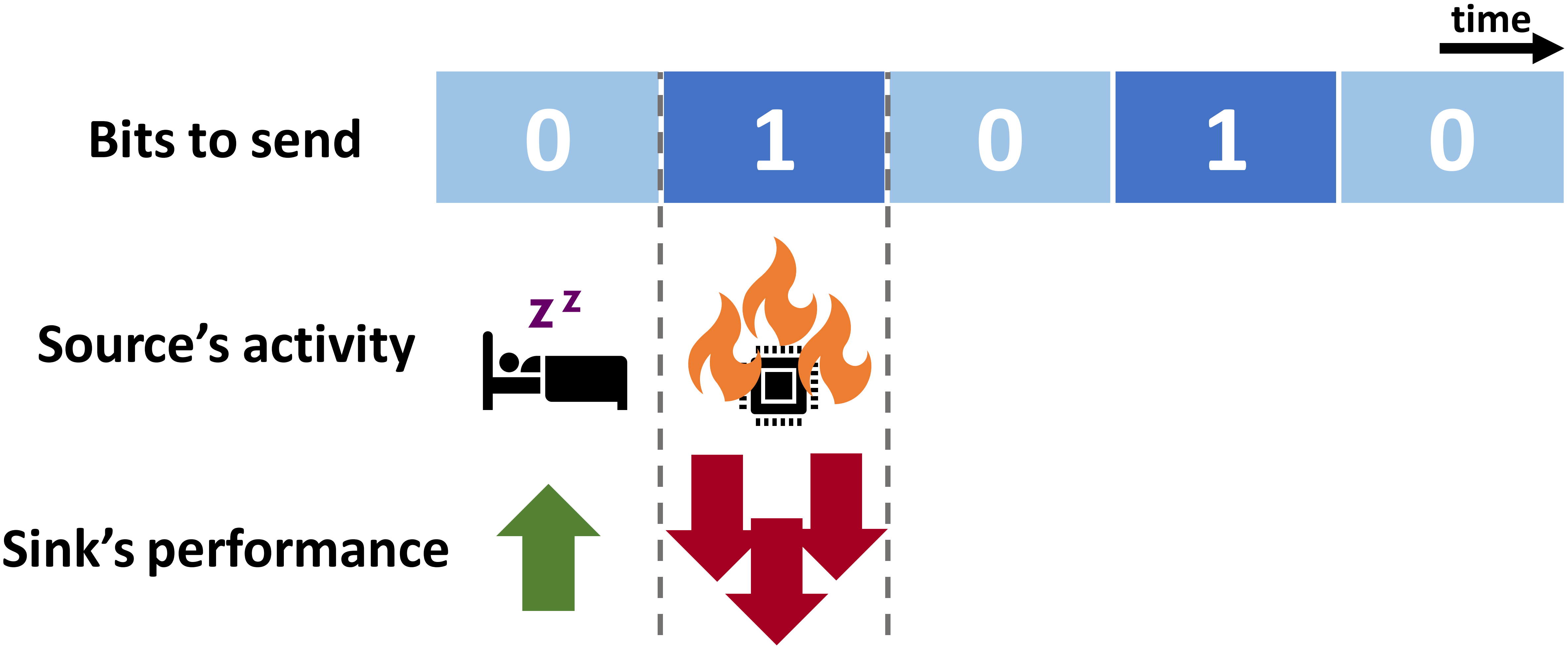
time

Bits to send	0	1	0	1	0

Source’s activity

Sink’s performance

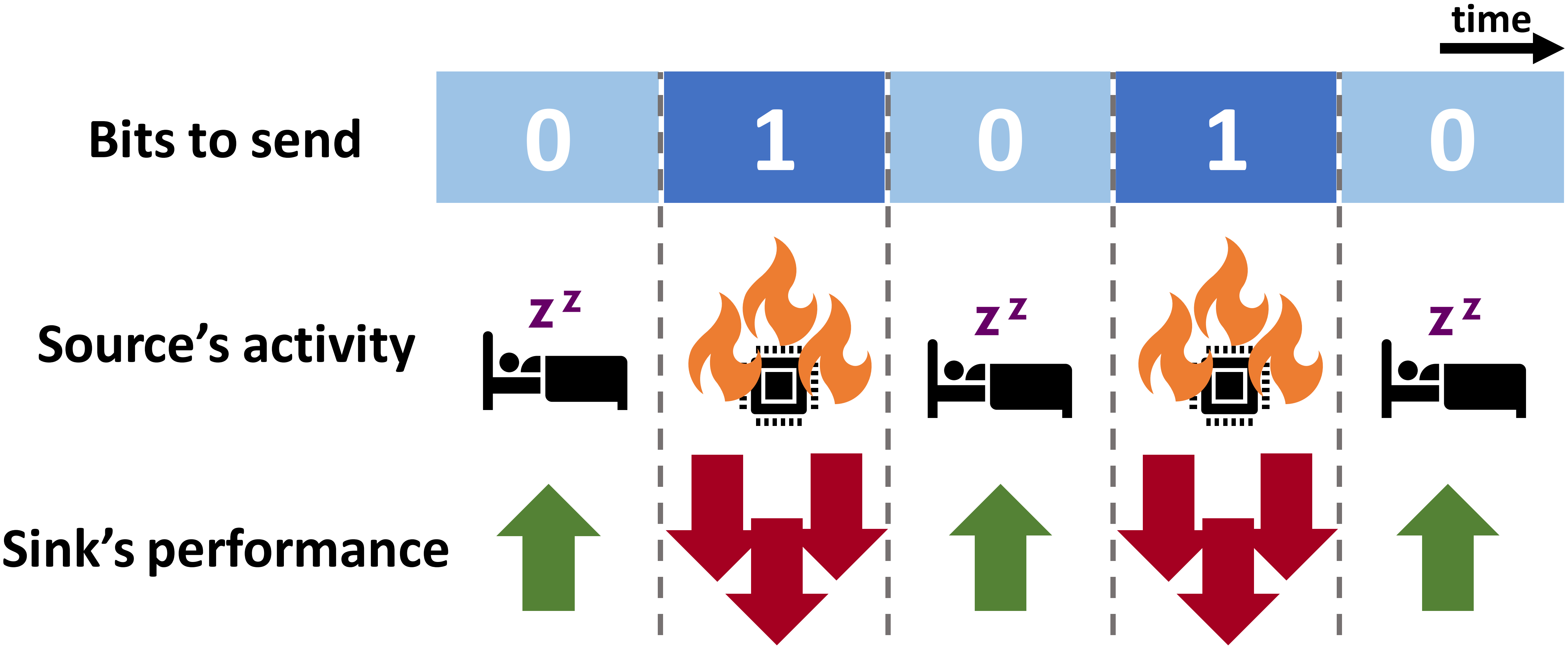
Stronger Single-bit Encoding



time →

Bits to send	0	1	0	1	0
Source’s activity					
Sink’s performance					

Stronger Single-bit Encoding



time

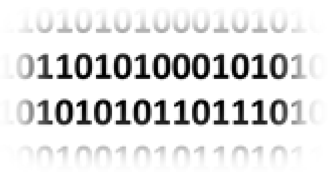
Bits to send

0 | 1 | 0 | 1 | 0

Source's activity

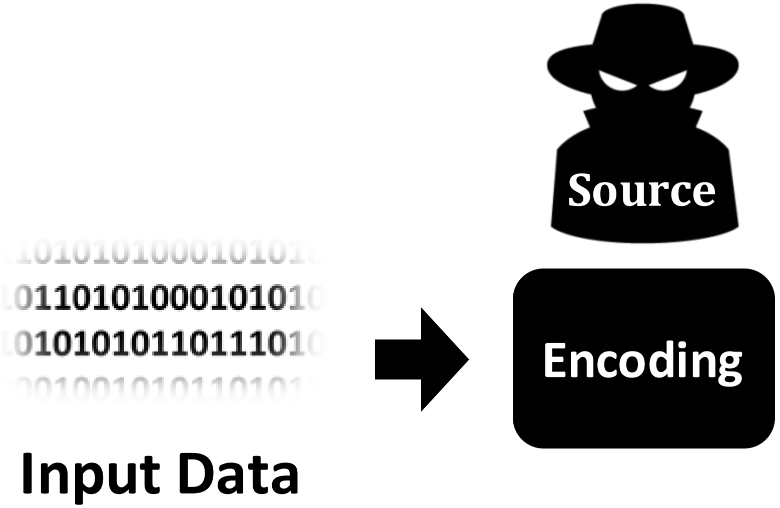
Sink's performance

Channel Characterization

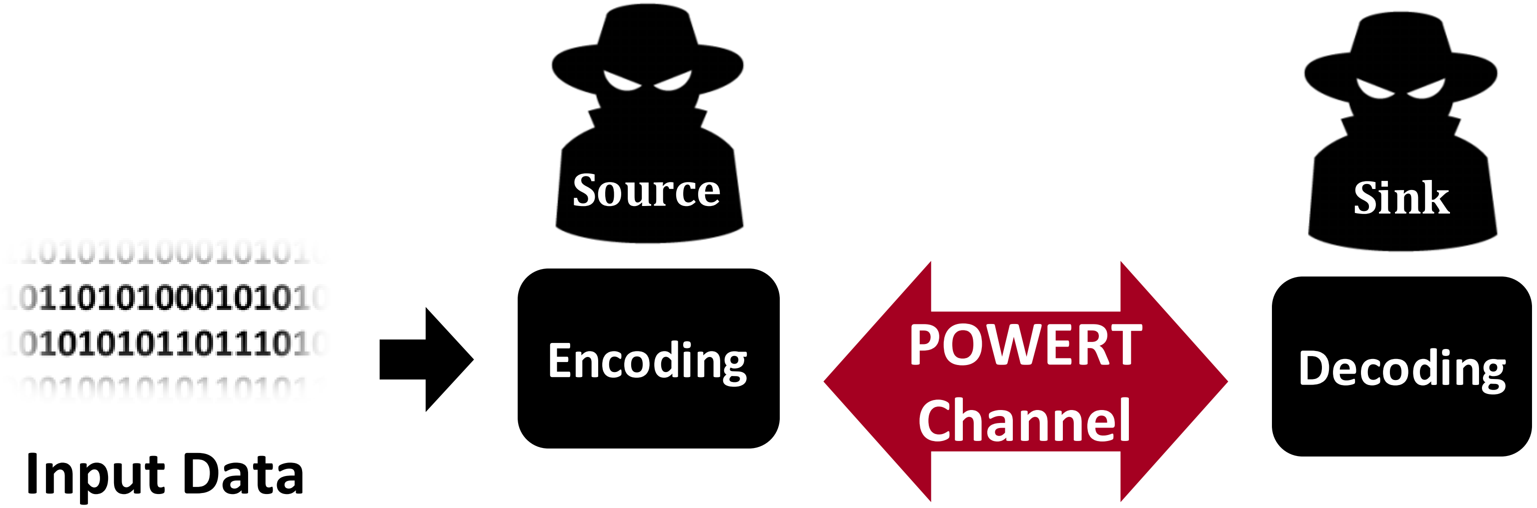


Input Data

Channel Characterization

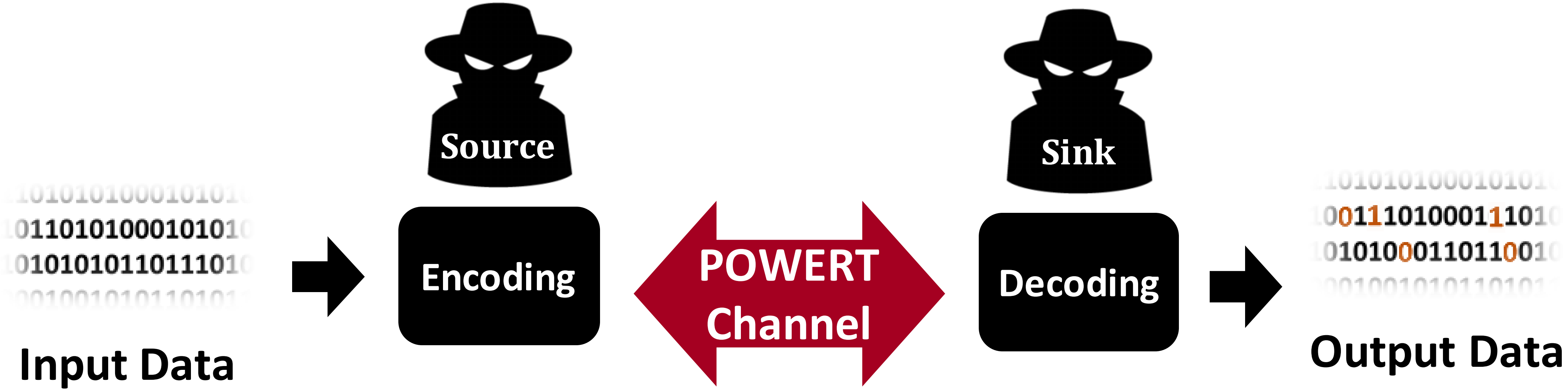


Channel Characterization



Input Data

Channel Characterization



Input Data

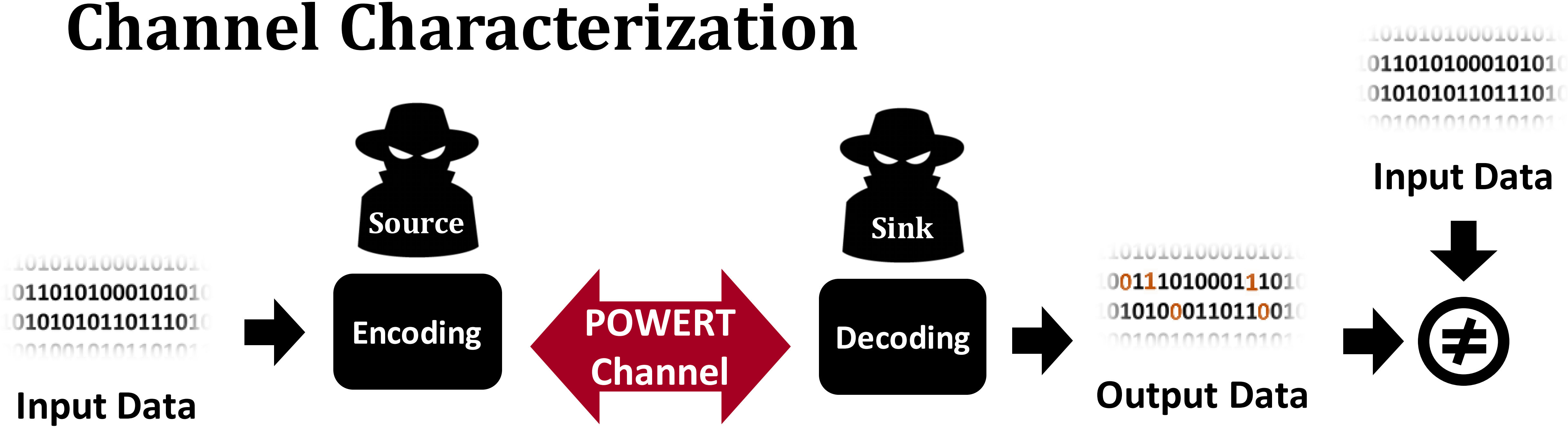
Encoding

POWERT Channel

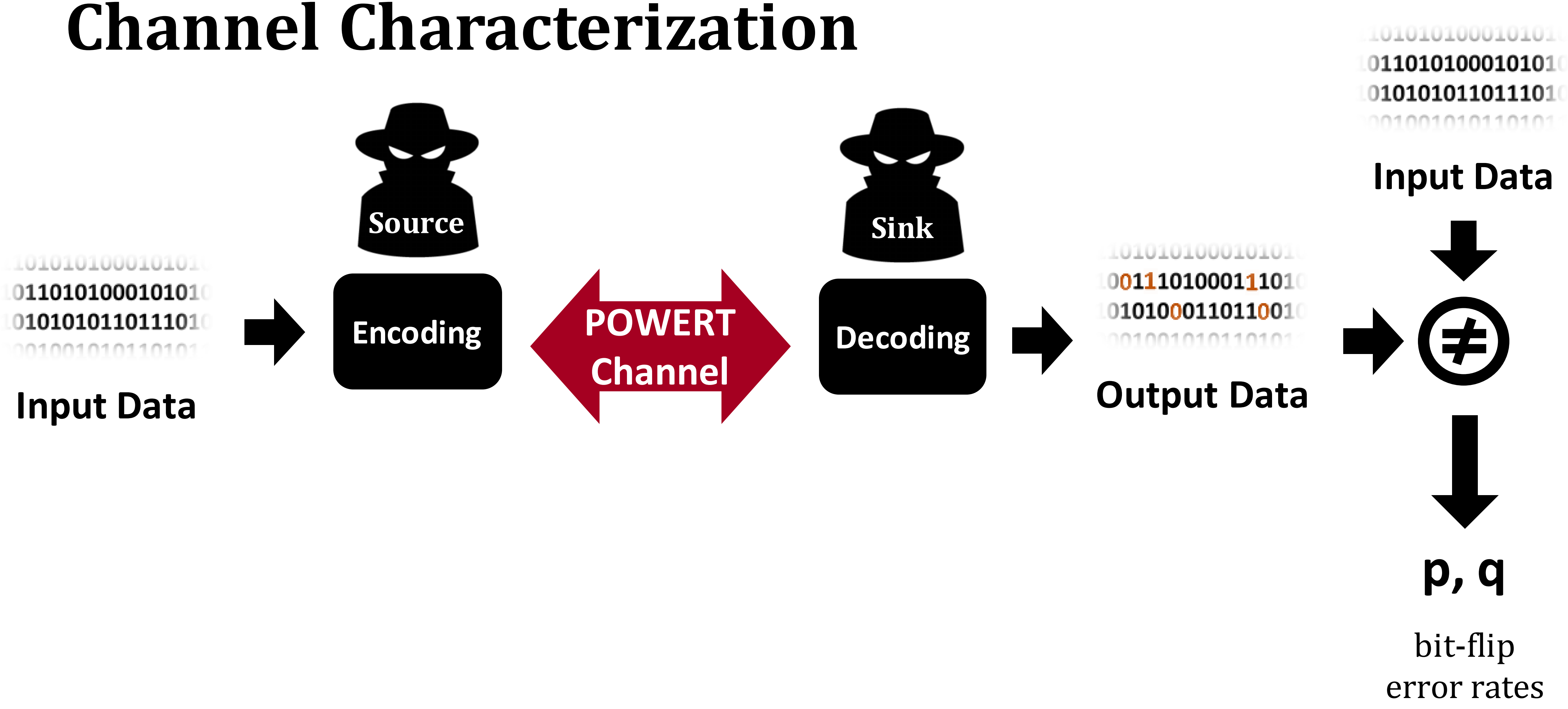
Decoding

Output Data

Channel Characterization



Channel Characterization



Input Data

Source

Encoding

POWERT Channel

Sink

Decoding

Output Data

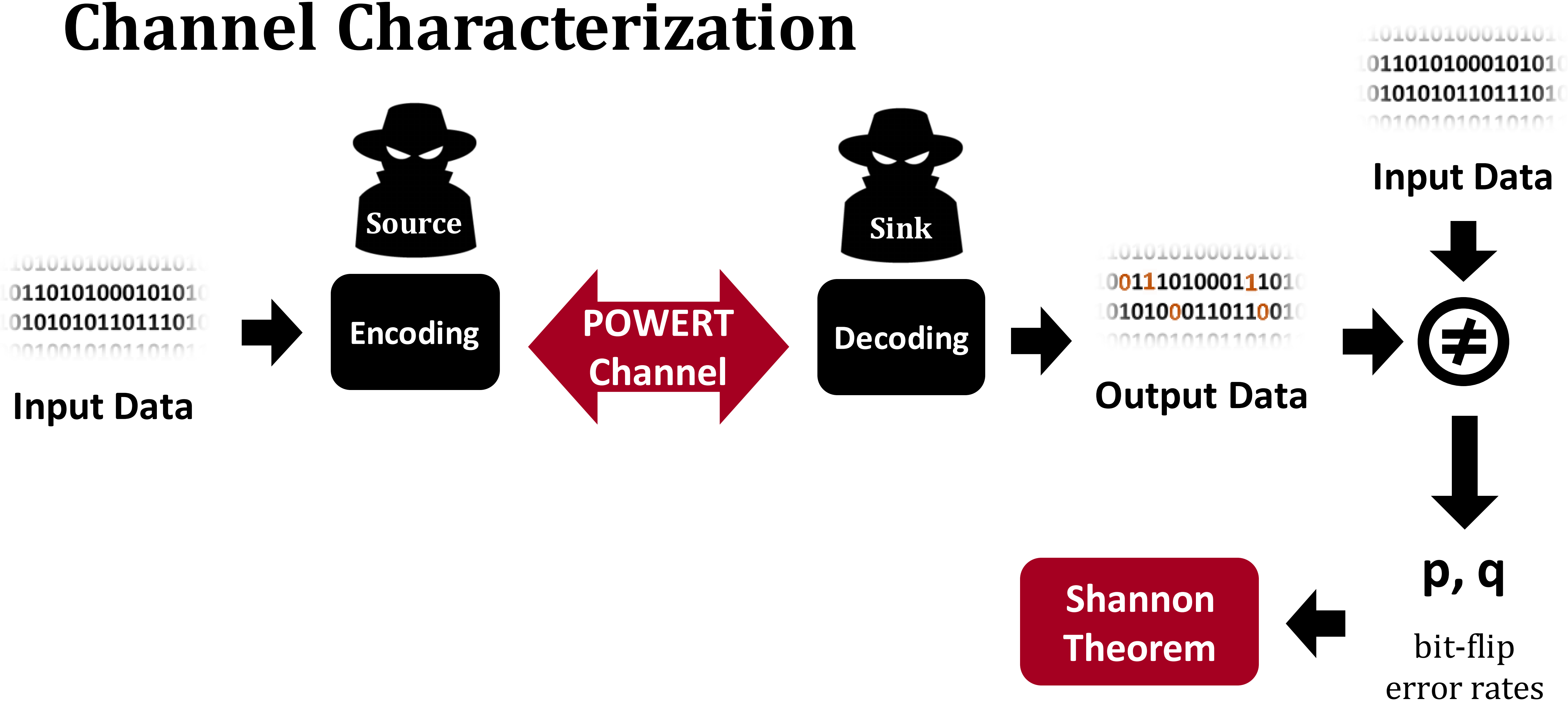
Input Data

≠

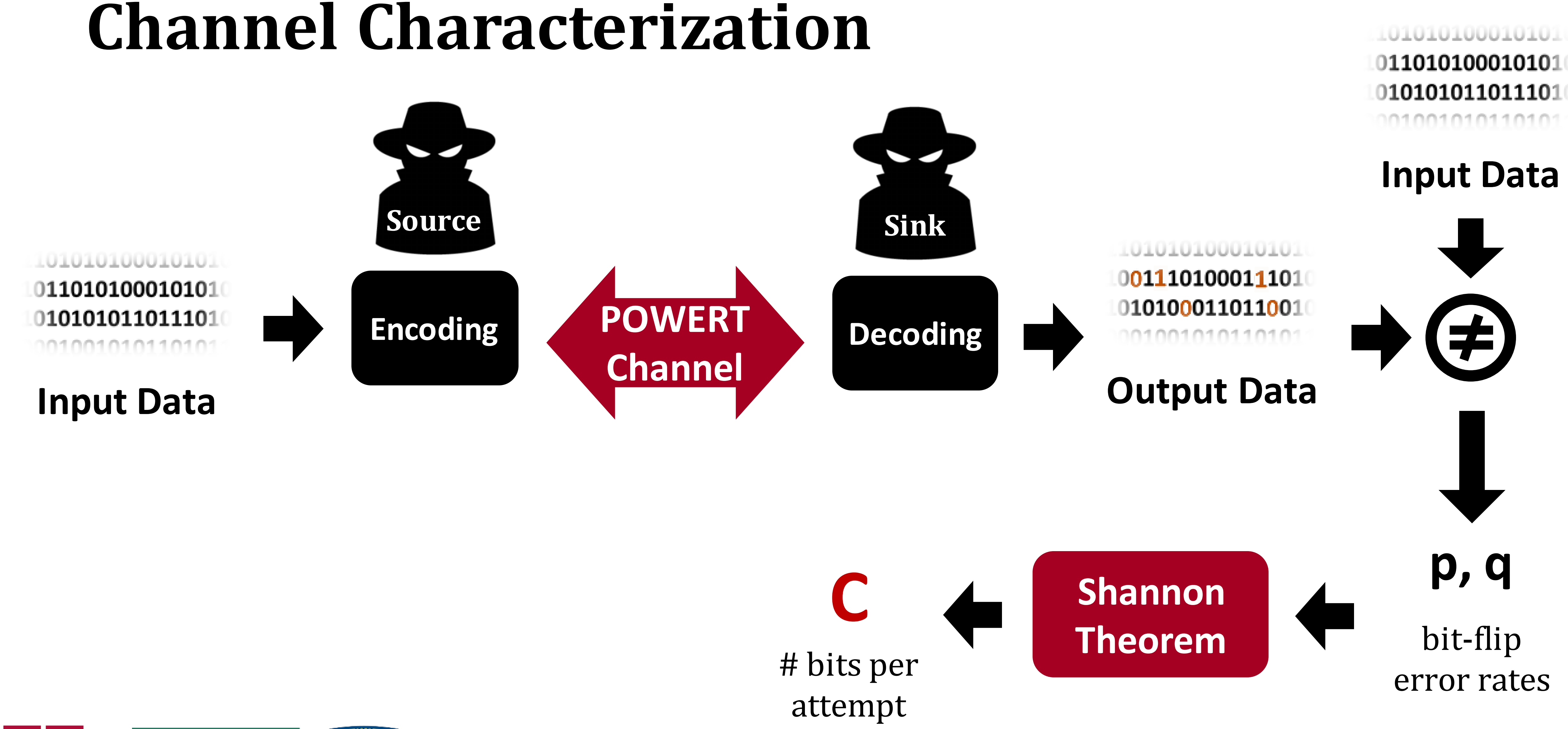
p, q

bit-flip error rates

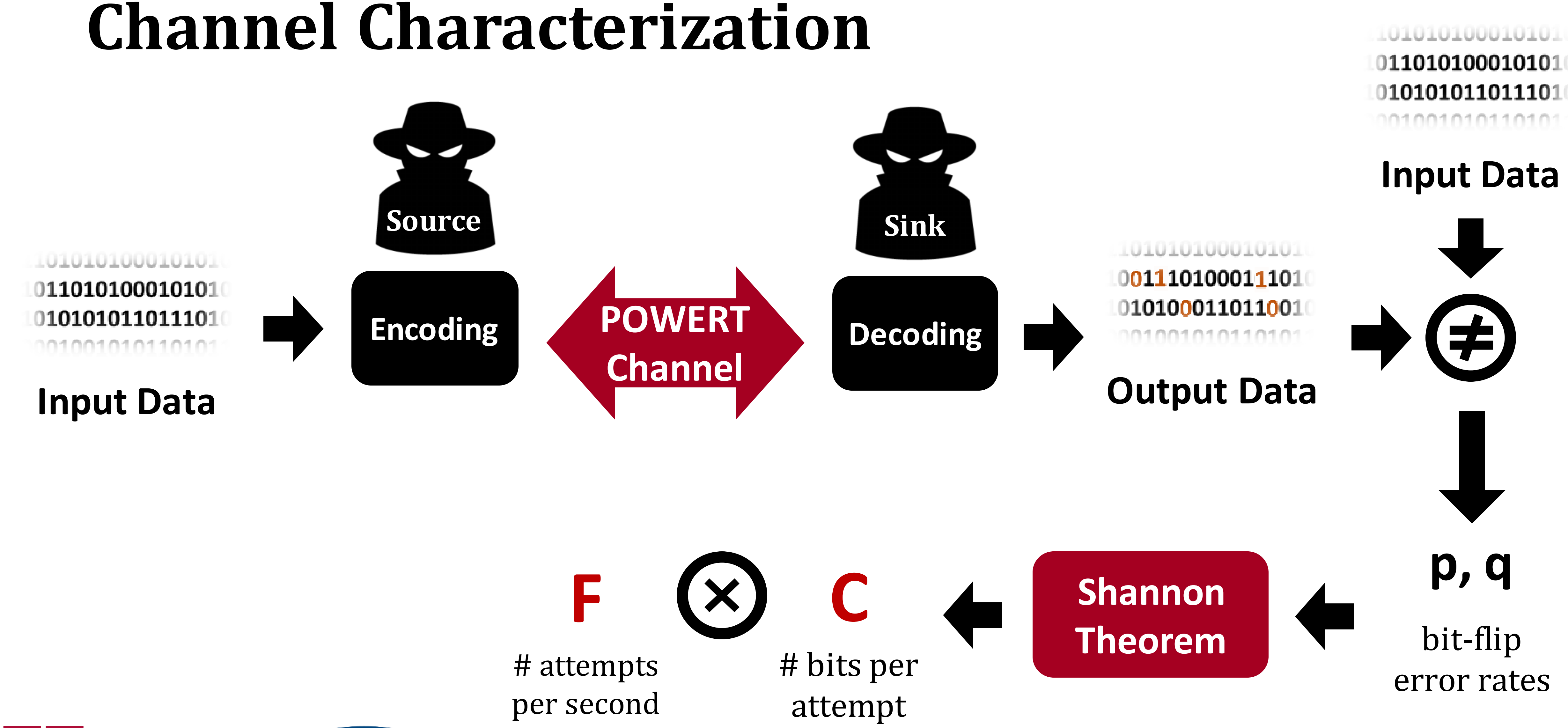
Channel Characterization



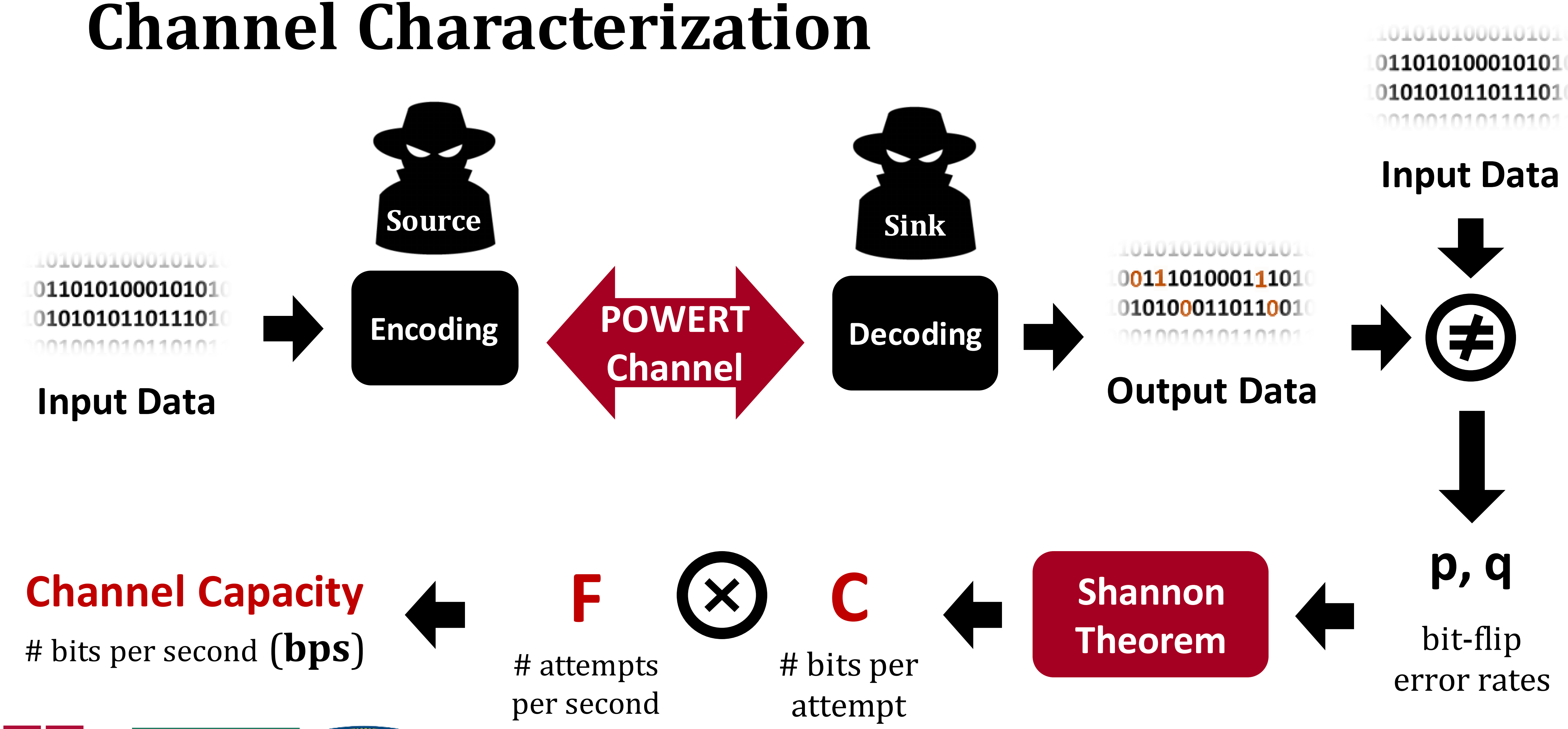
Channel Characterization



Channel Characterization



Channel Characterization



Source

Sink

Input Data

Encoding

POWERT Channel

Decoding

Output Data

Input Data

≠

p, q

bit-flip error rates

Shannon Theorem

C

# bits per attempt

⊗

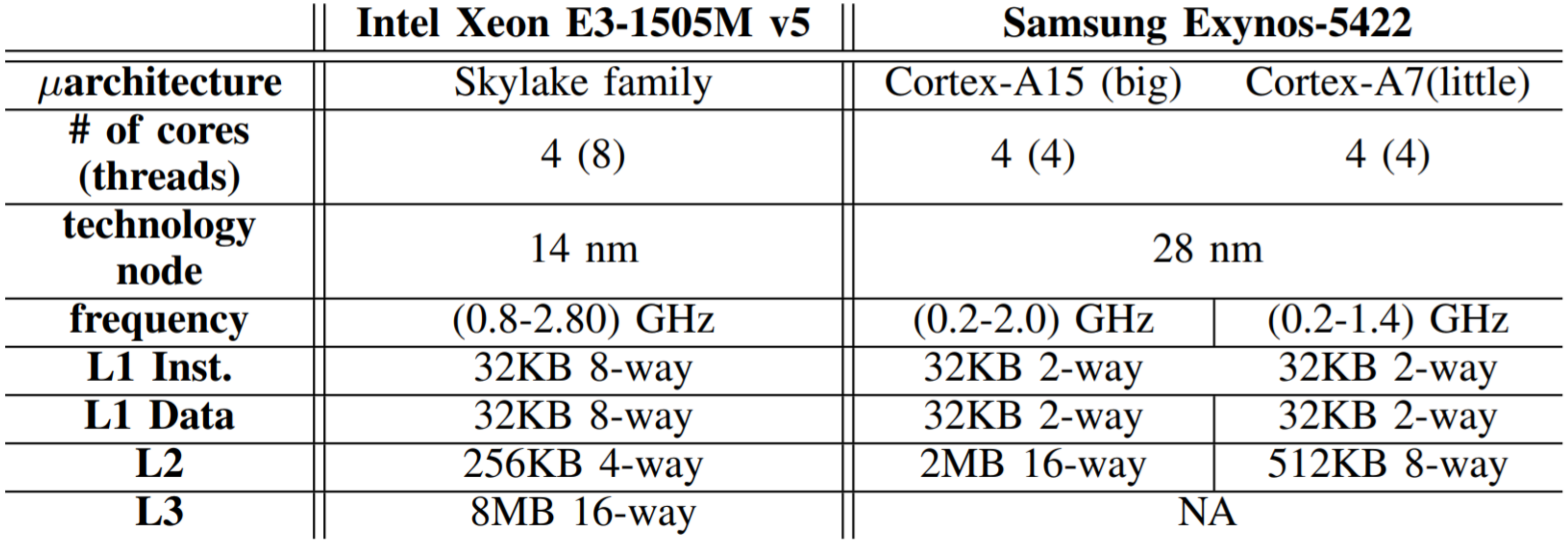
F

# attempts per second

Channel Capacity

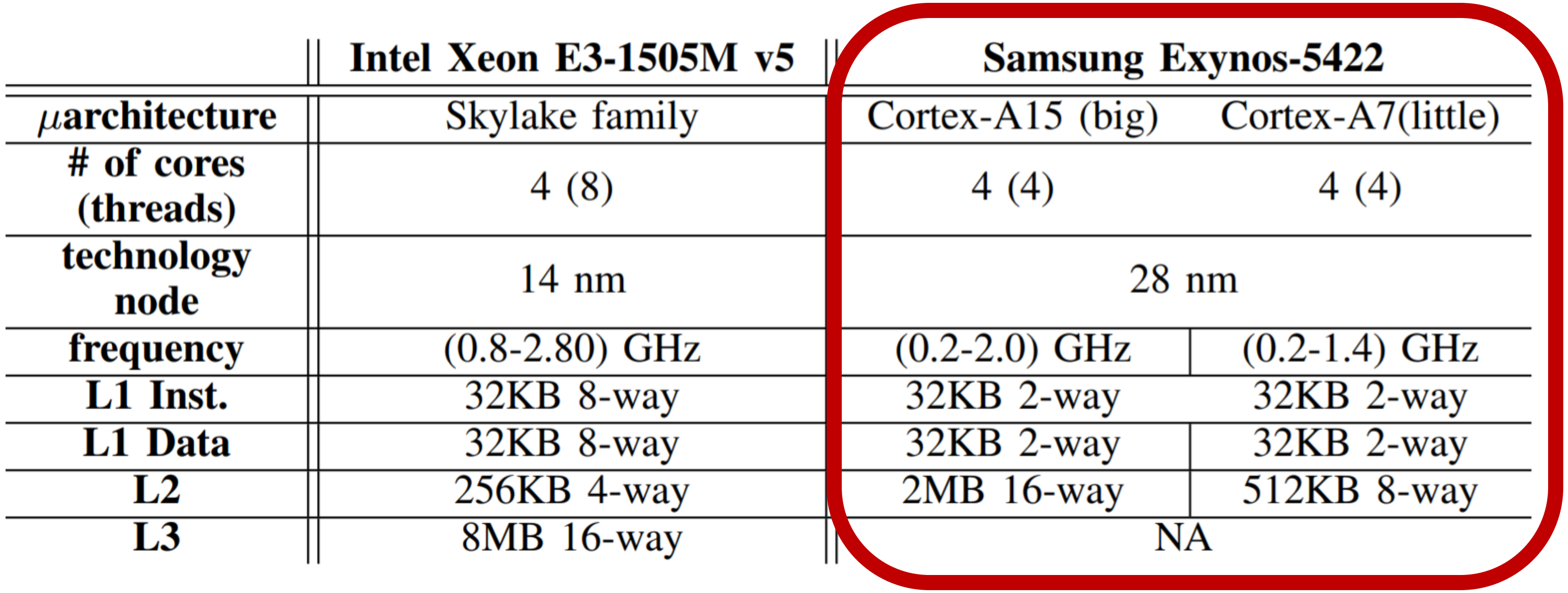
# bits per second (**bps**)

Evaluation Setup



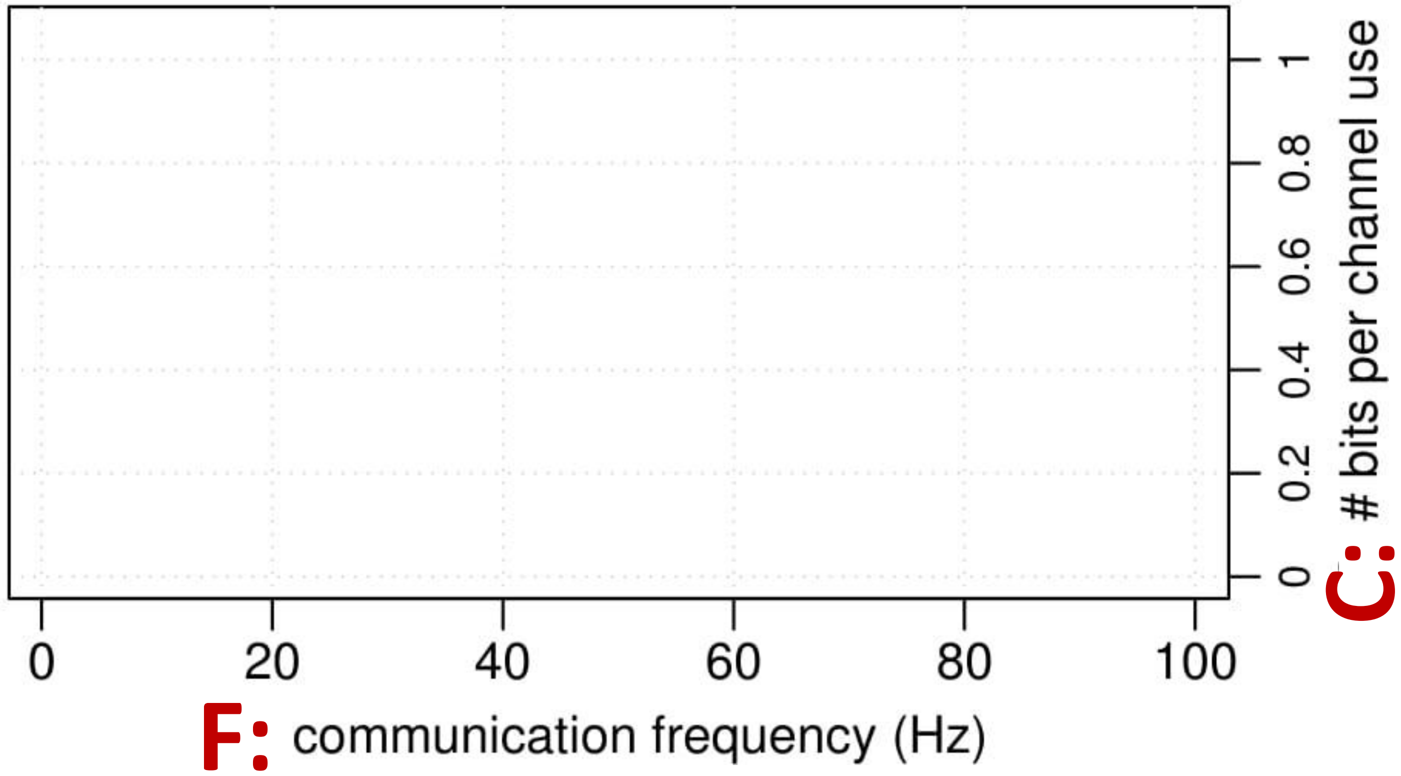
	Intel Xeon E3-1505M v5	**Samsung Exynos-5422**	
μarchitecture	Skylake family	Cortex-A15 (big)	Cortex-A7(little)
# of cores (threads)	4 (8)	4 (4)	4 (4)
technology node	14 nm	28 nm	
frequency	(0.8-2.80) GHz	(0.2-2.0) GHz	(0.2-1.4) GHz
L1 Inst.	32KB 8-way	32KB 2-way	32KB 2-way
L1 Data	32KB 8-way	32KB 2-way	32KB 2-way
L2	256KB 4-way	2MB 16-way	512KB 8-way
L3	8MB 16-way	NA	

Evaluation Setup

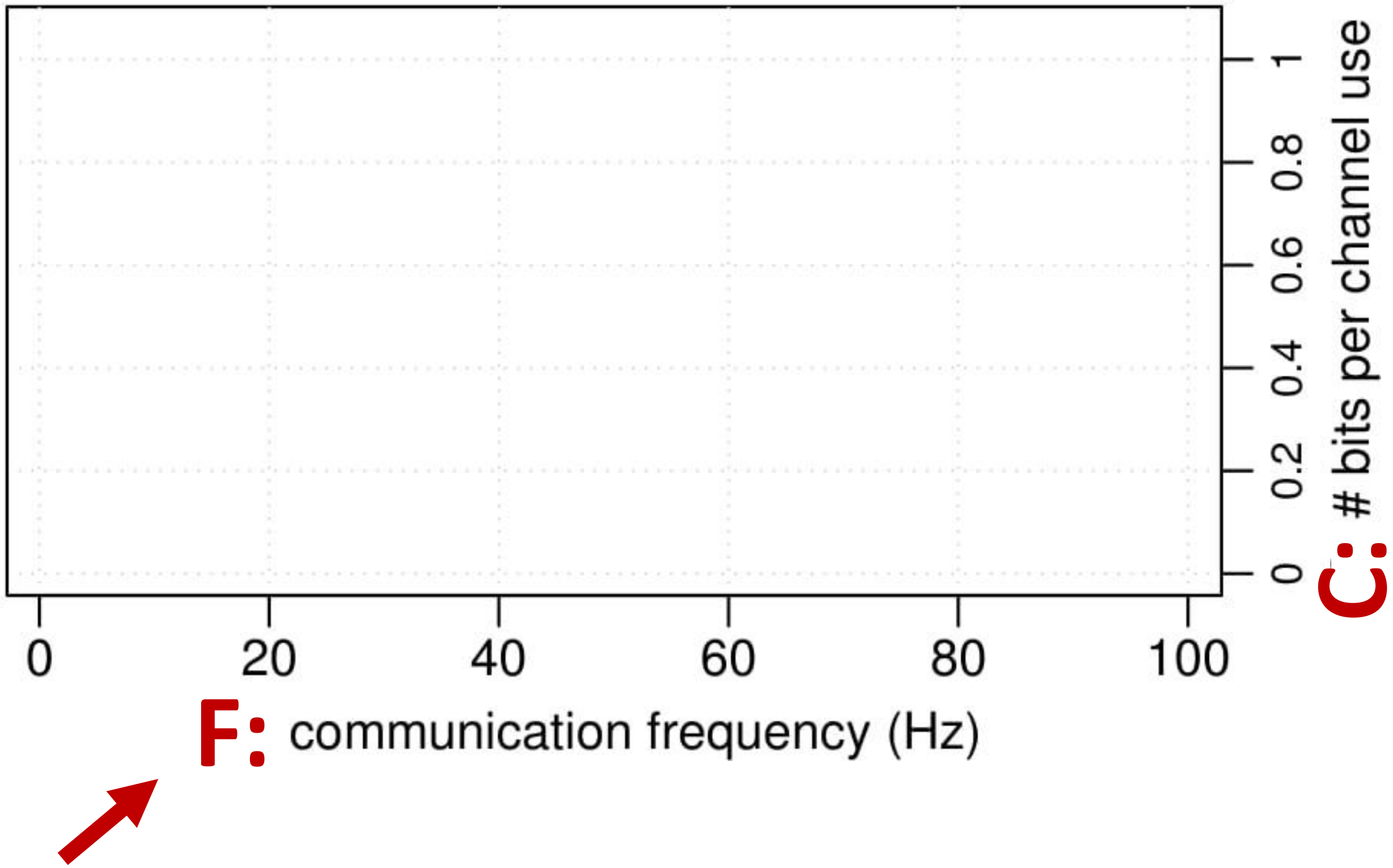


	Intel Xeon E3-1505M v5	Samsung Exynos-5422	
μarchitecture	Skylake family	Cortex-A15 (big)	Cortex-A7(little)
# of cores (threads)	4 (8)	4 (4)	4 (4)
technology node	14 nm	28 nm	
frequency	(0.8-2.80) GHz	(0.2-2.0) GHz	(0.2-1.4) GHz
L1 Inst.	32KB 8-way	32KB 2-way	32KB 2-way
L1 Data	32KB 8-way	32KB 2-way	32KB 2-way
L2	256KB 4-way	2MB 16-way	512KB 8-way
L3	8MB 16-way	NA	

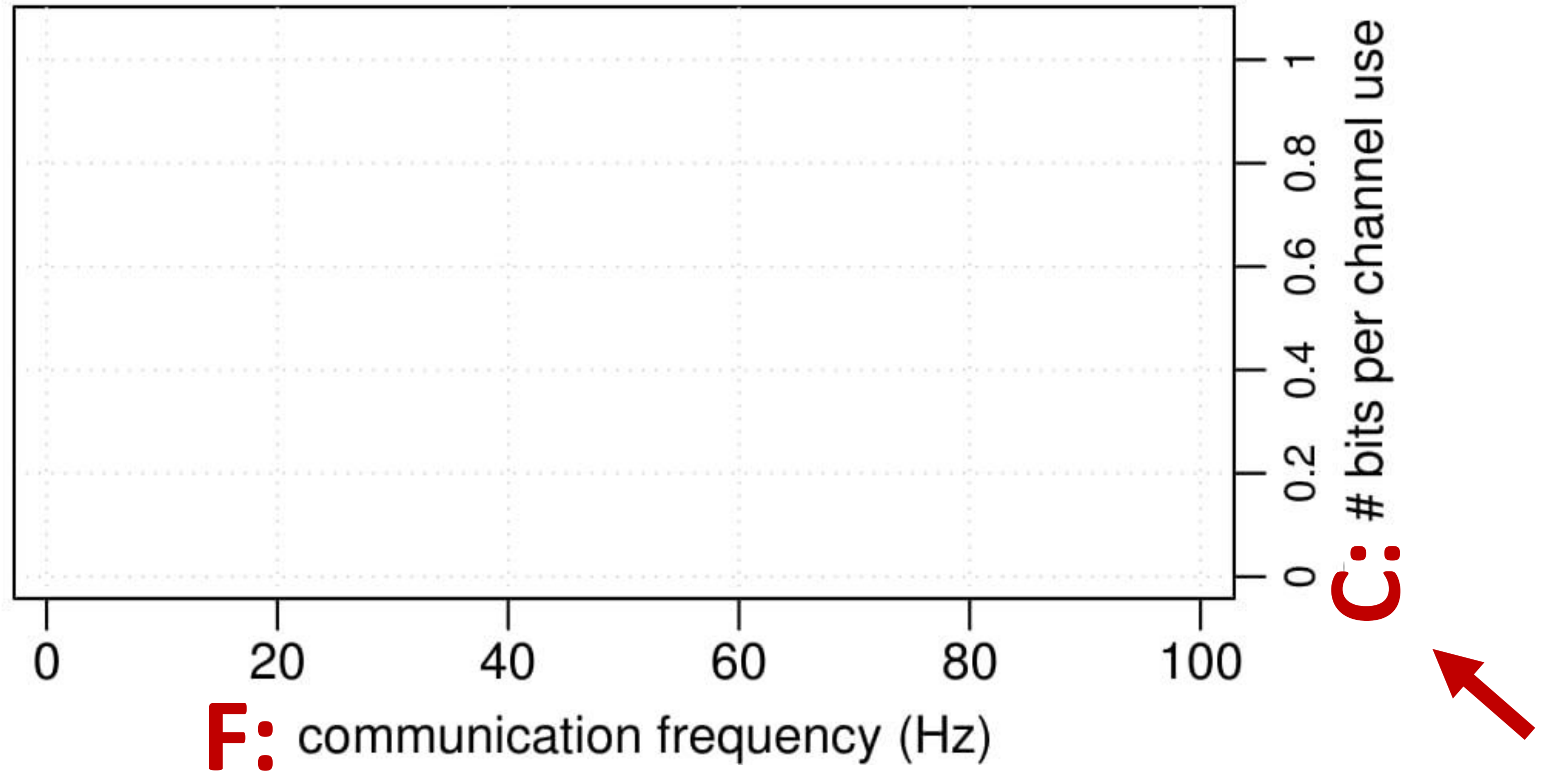
Channel Capacity: Single-bit Encoding



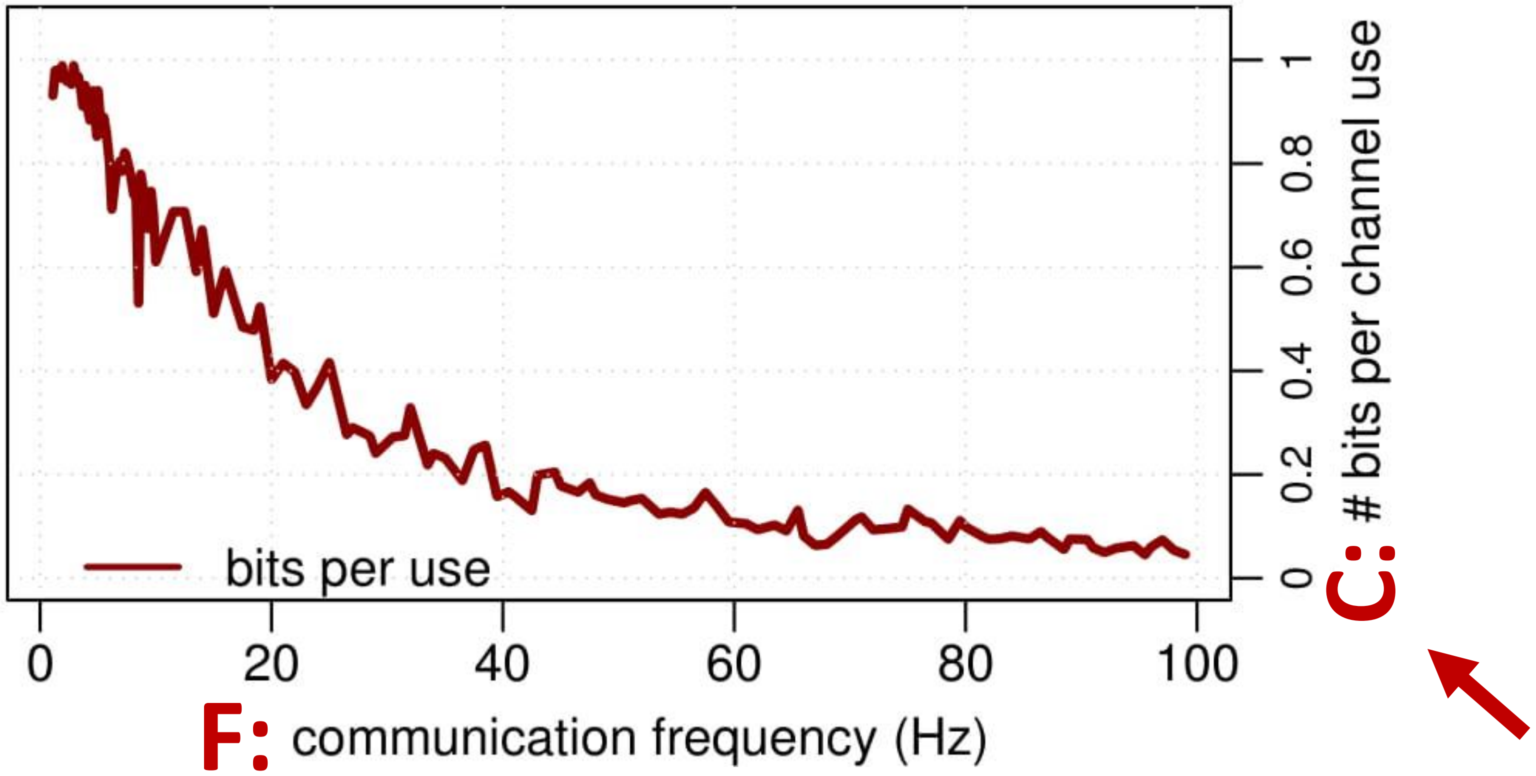
Channel Capacity: Single-bit Encoding



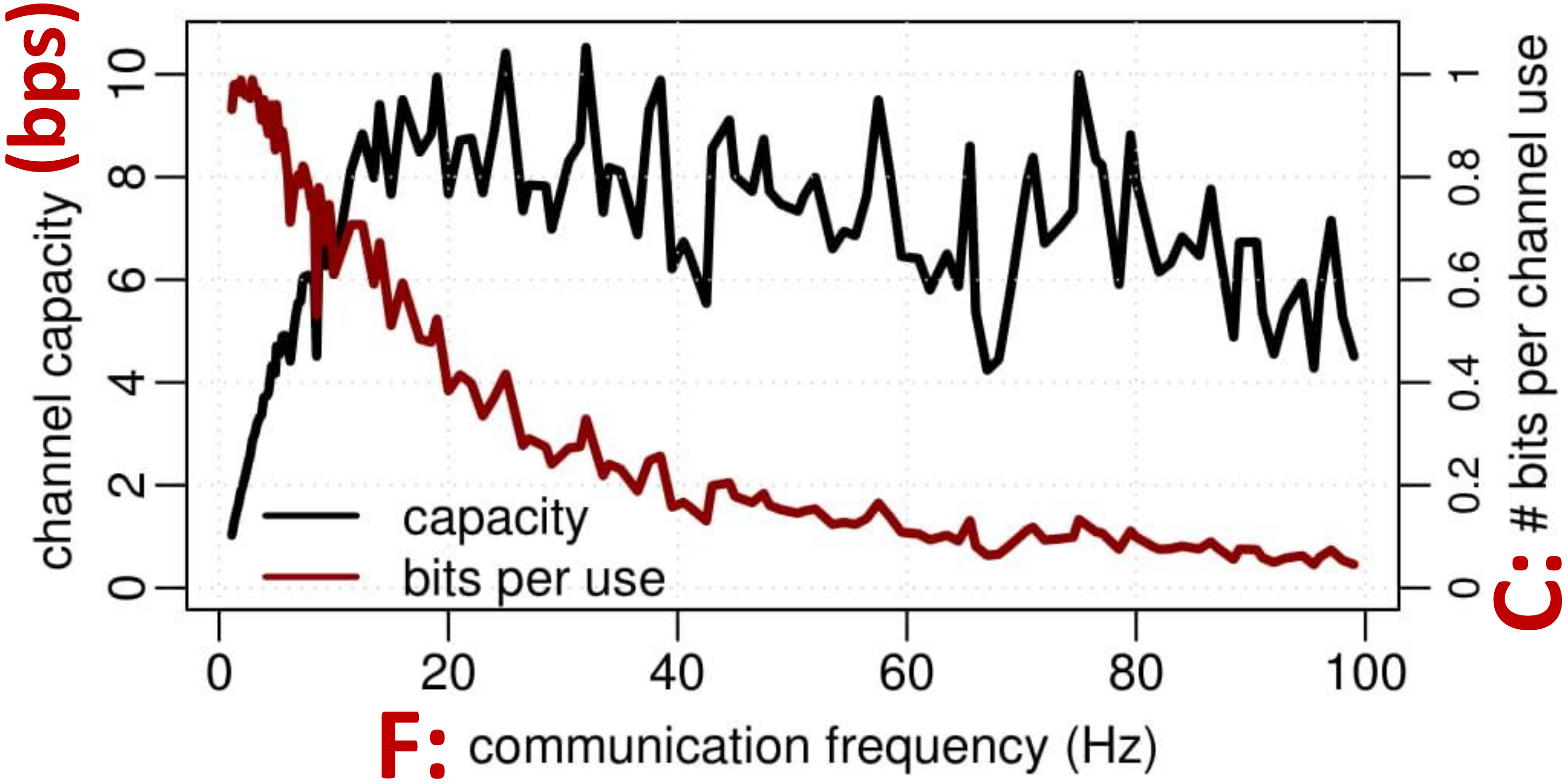
Channel Capacity: Single-bit Encoding



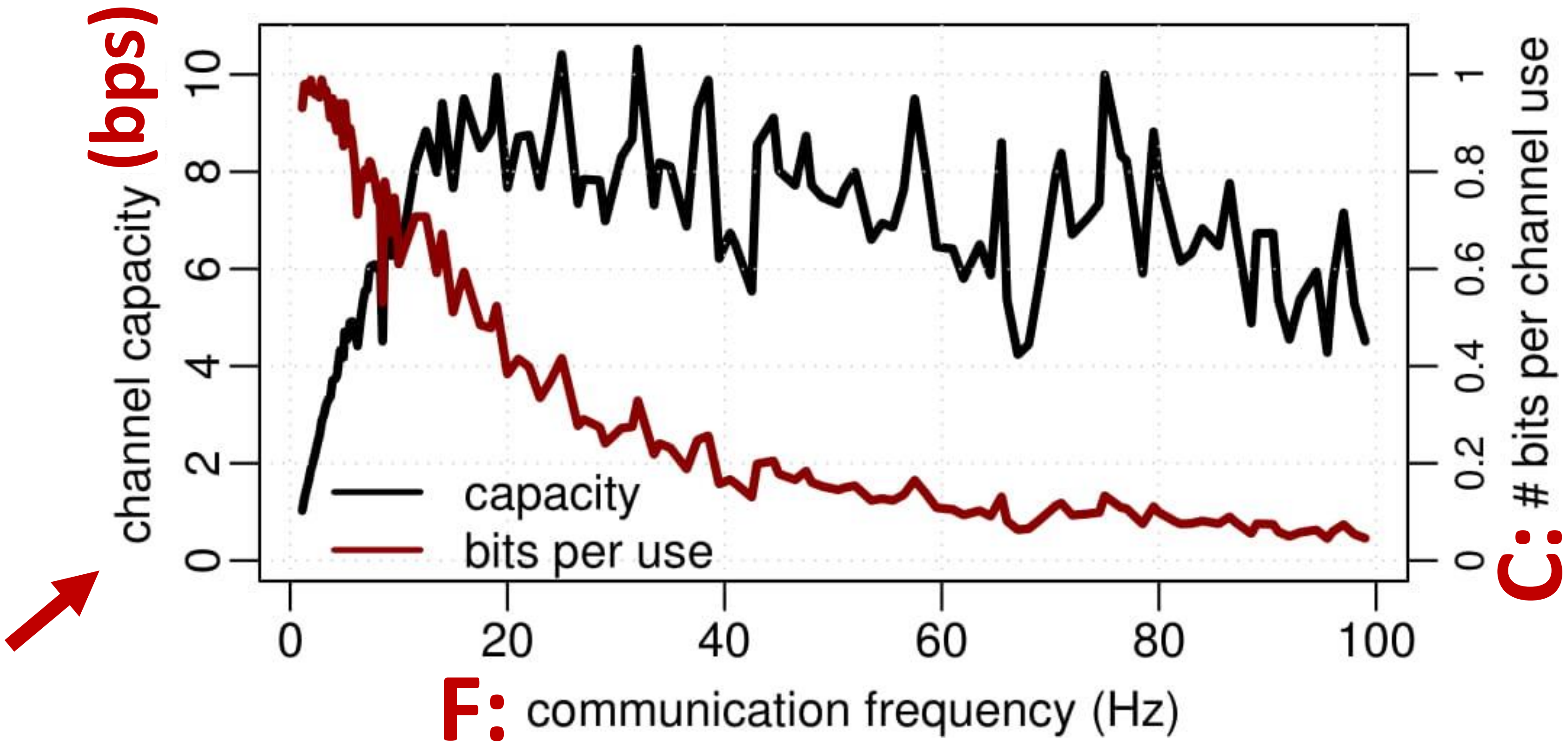
Channel Capacity: Single-bit Encoding



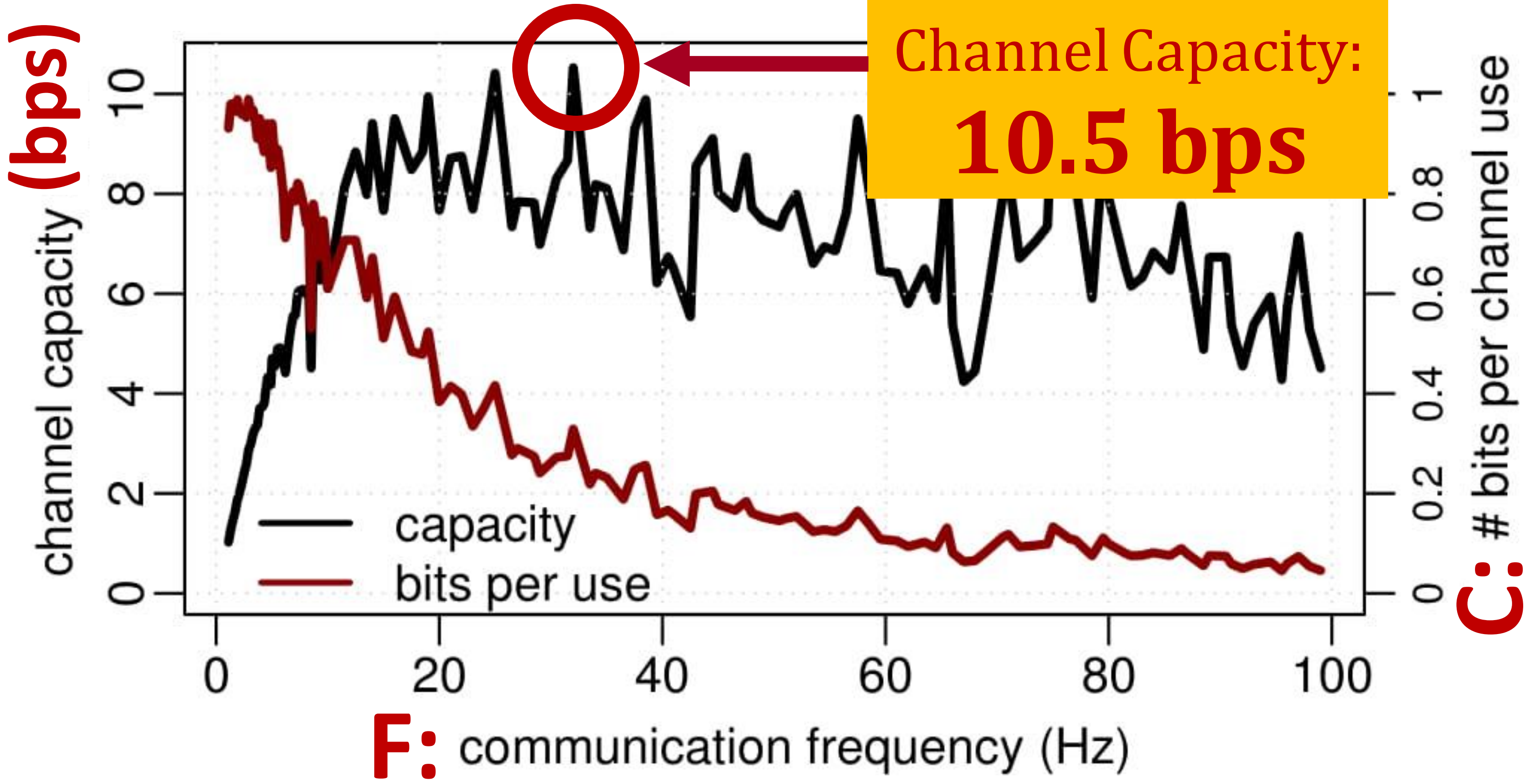
Channel Capacity: Single-bit Encoding



Channel Capacity: Single-bit Encoding

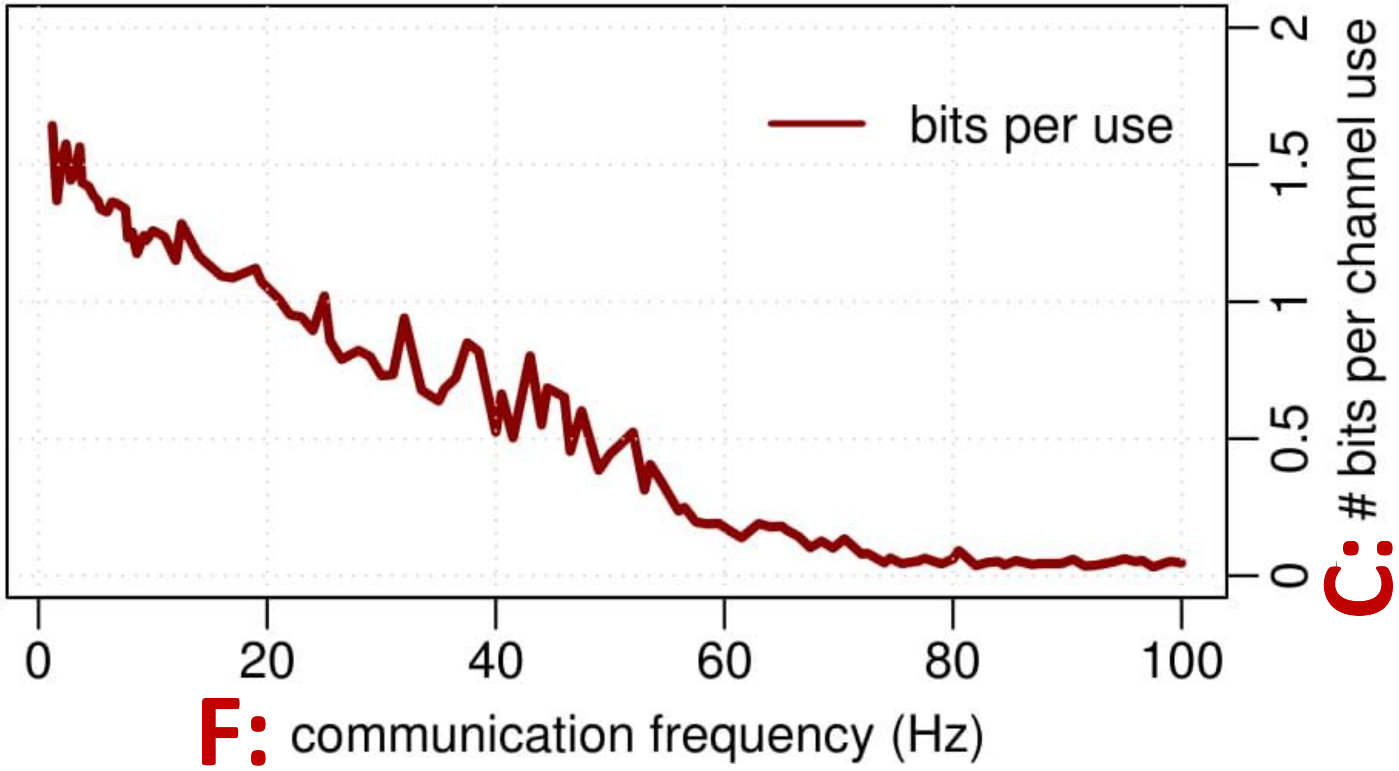


Channel Capacity: Single-bit Encoding

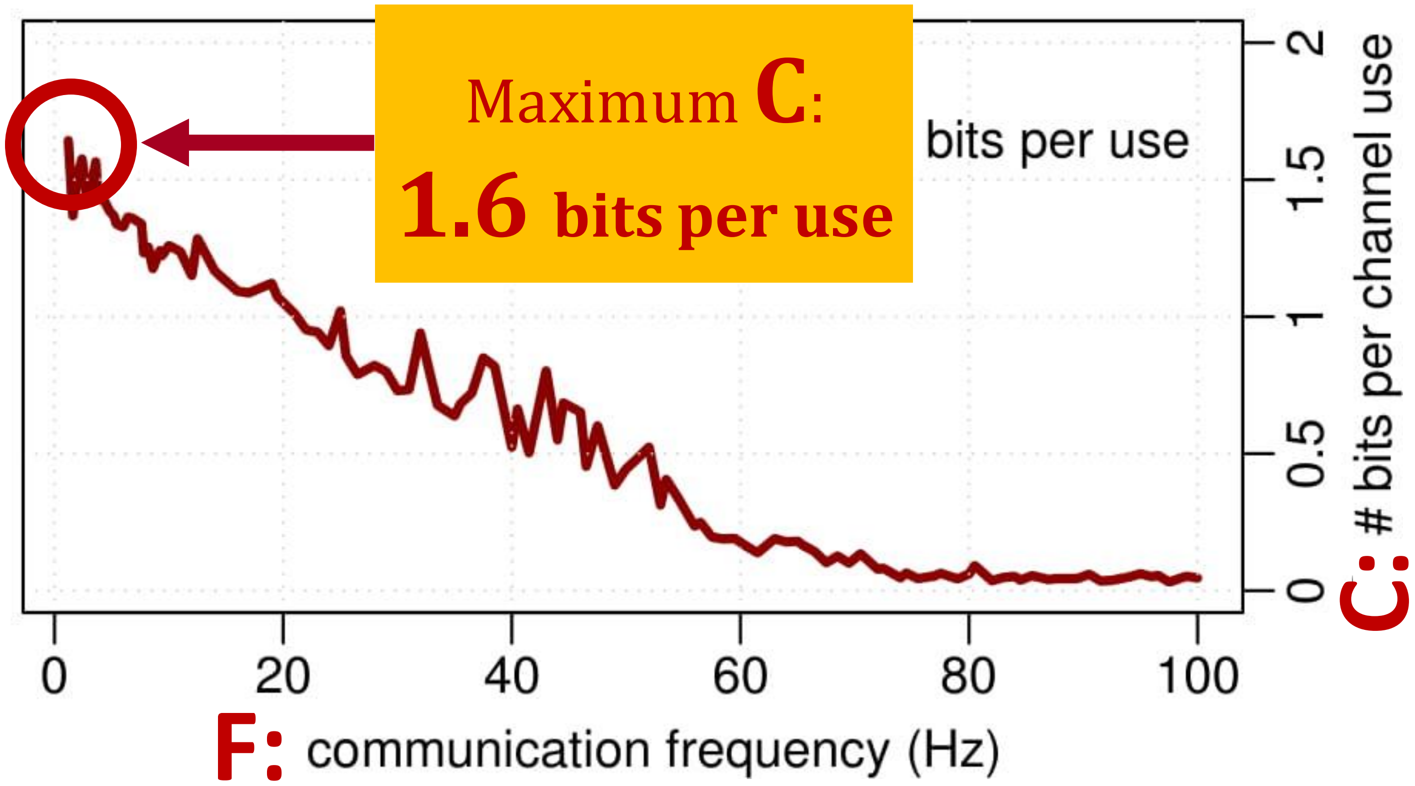


Maximum Channel Capacity: **10.5 bps**

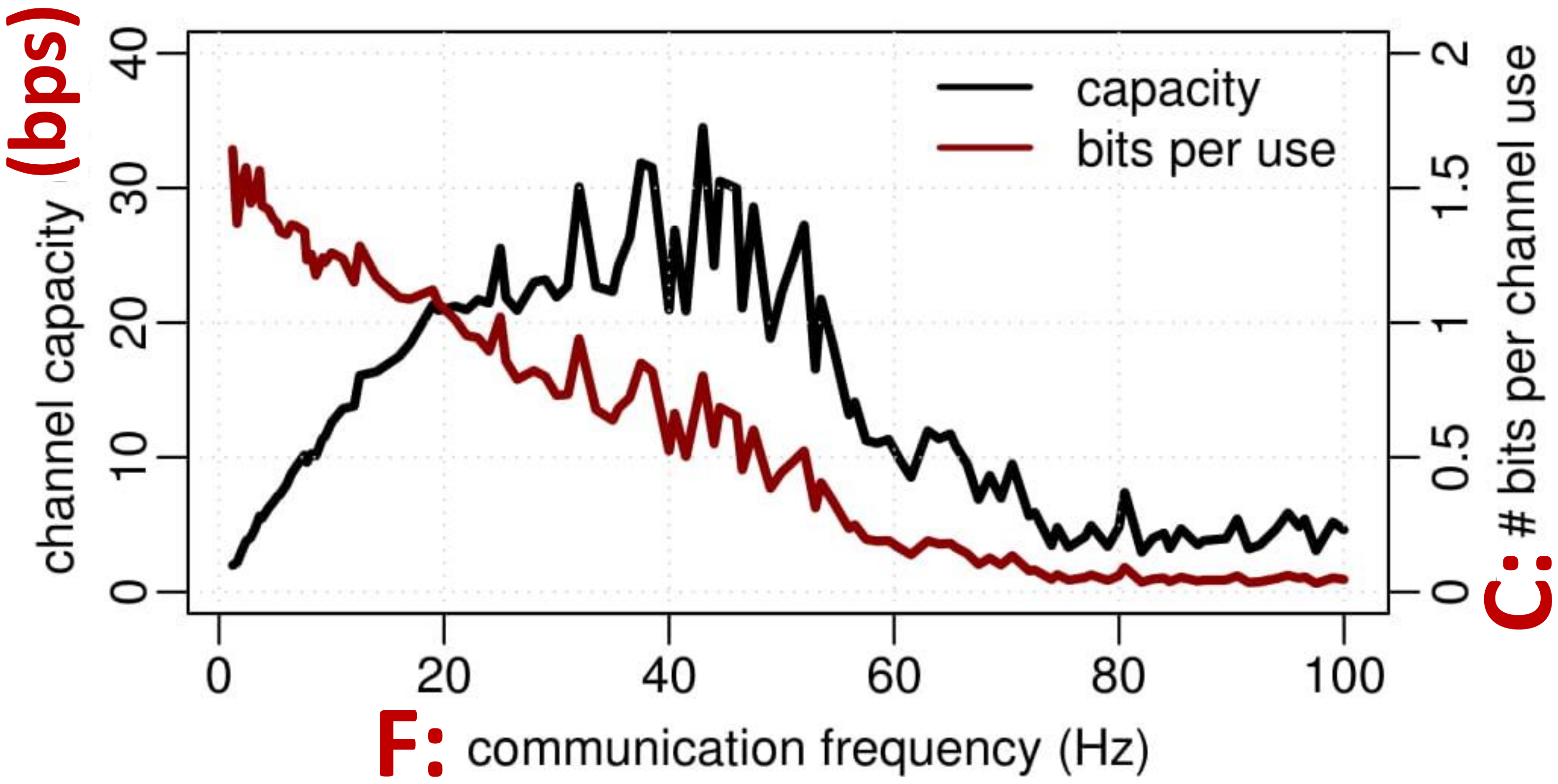
Channel Capacity: 2-bit Encoding



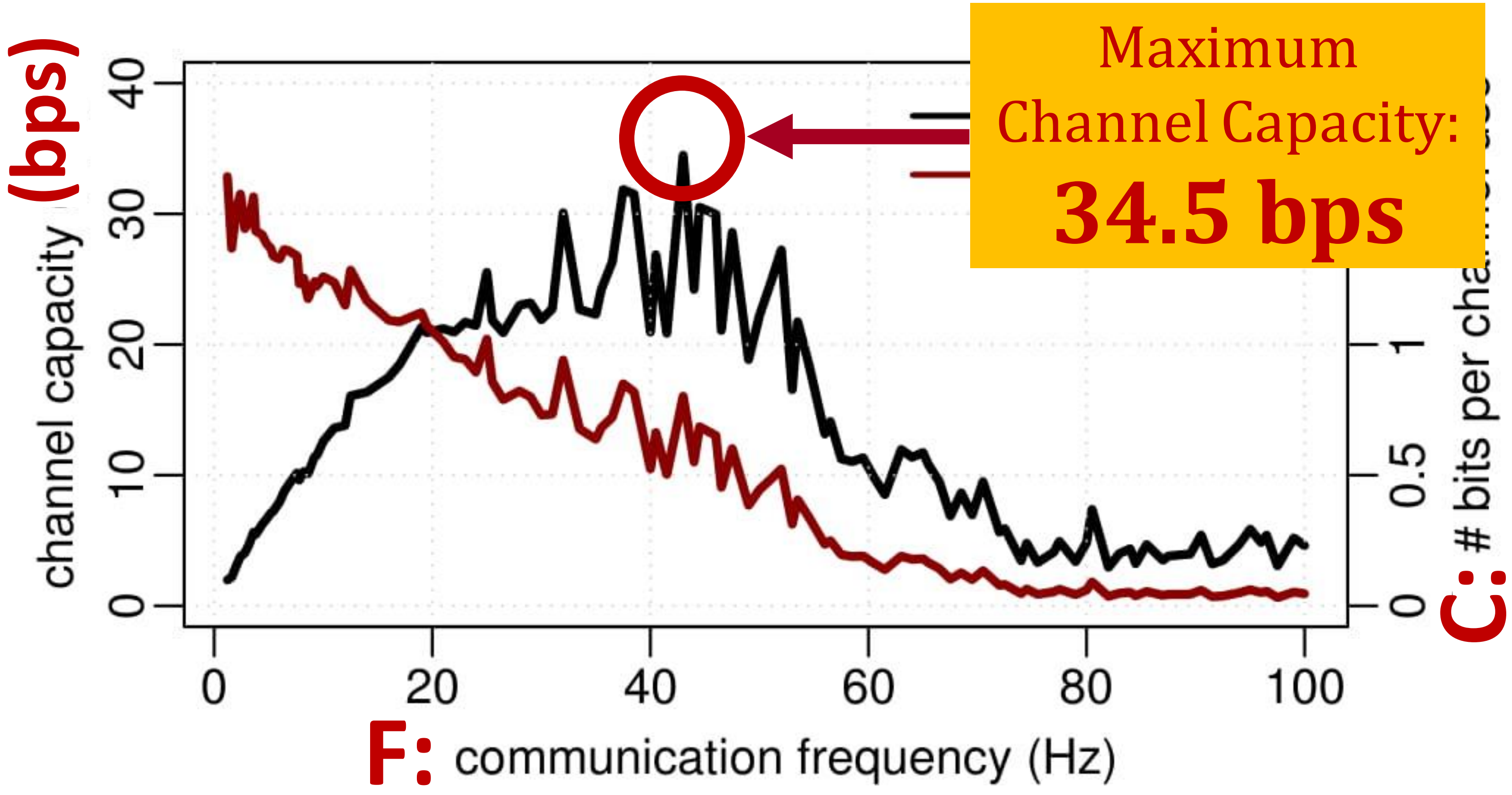
Channel Capacity: 2-bit Encoding



Channel Capacity: 2-bit Encoding

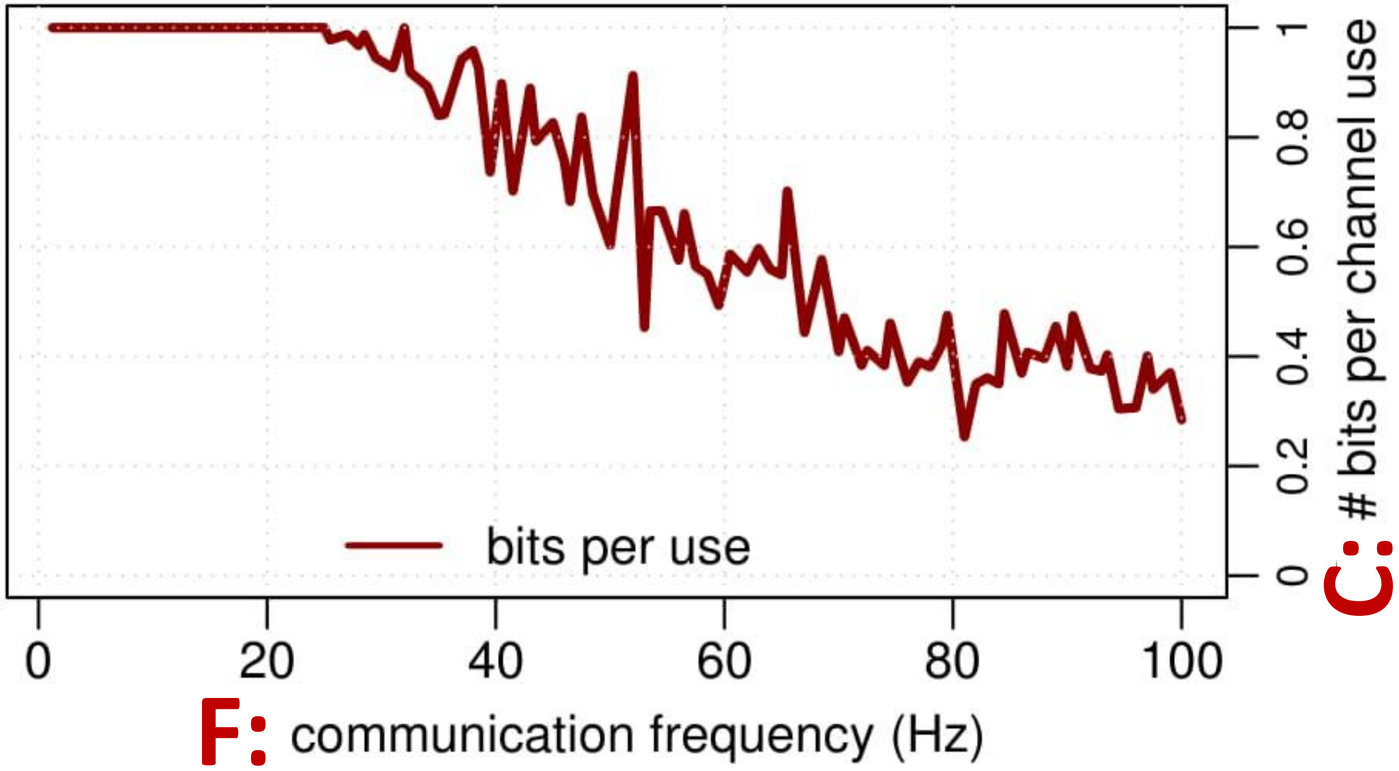


Channel Capacity: 2-bit Encoding

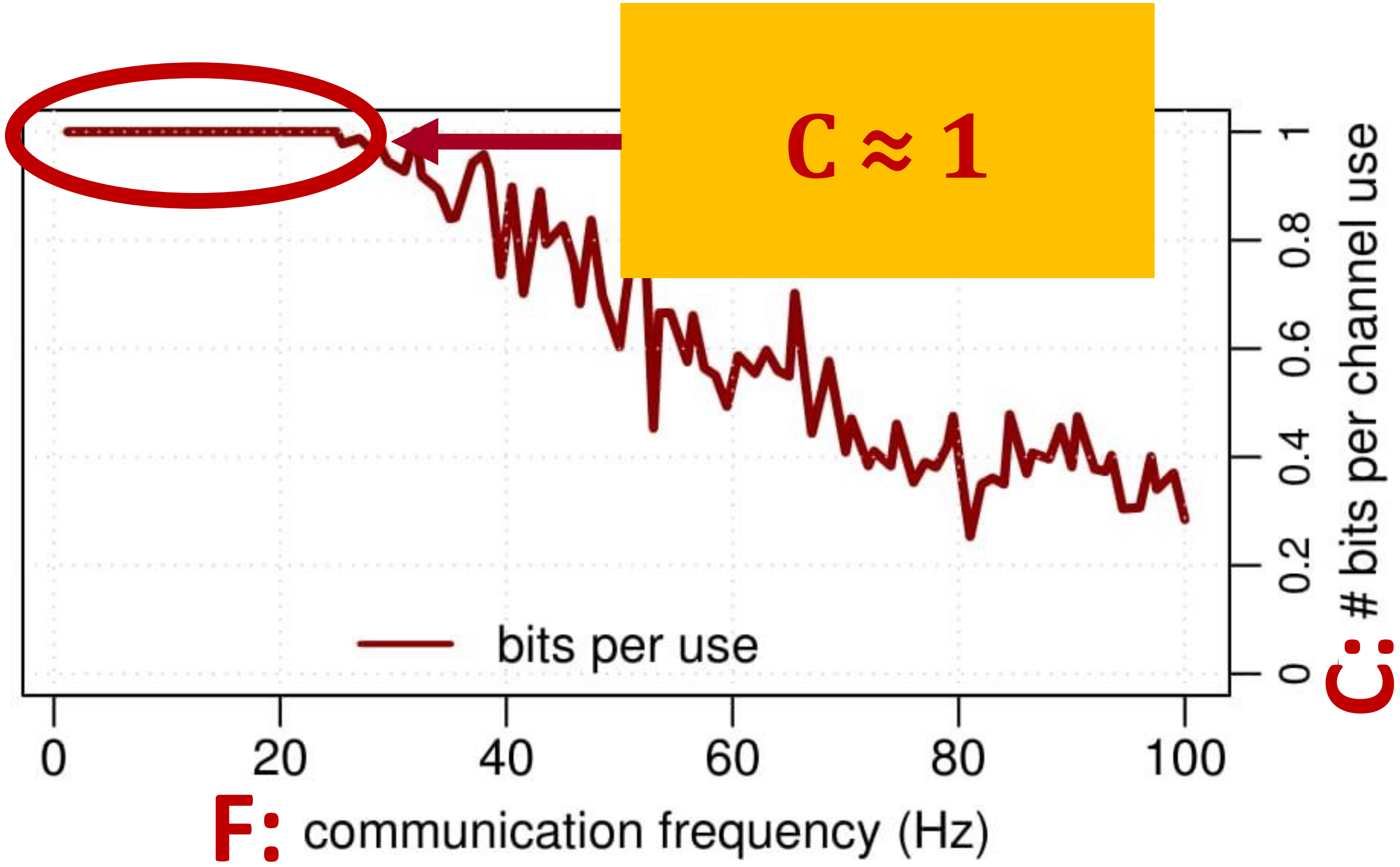


Maximum
Channel Capacity:
34.5 bps

Channel Capacity: Stronger Single-bit Encoding

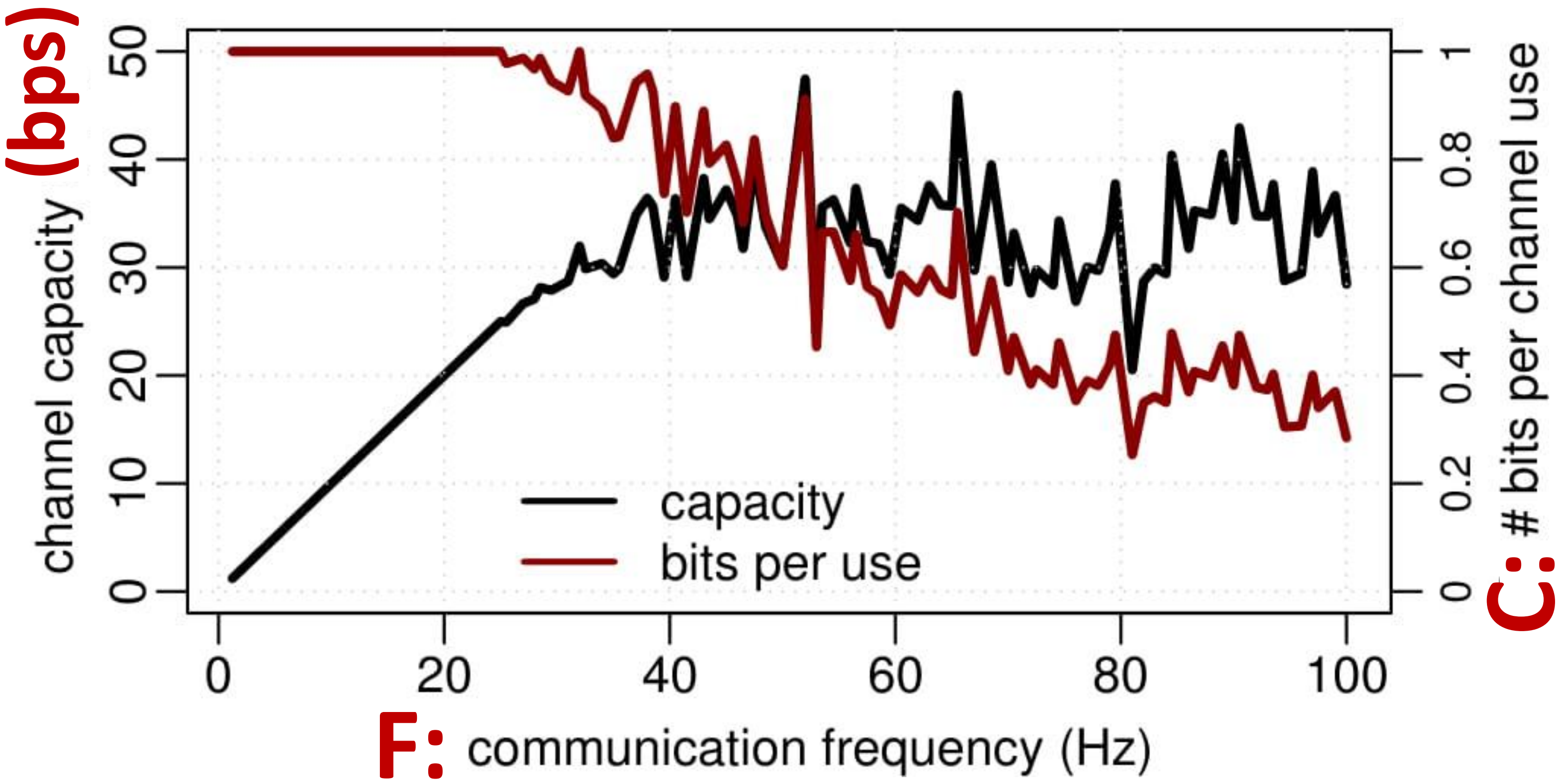


Channel Capacity: Stronger Single-bit Encoding

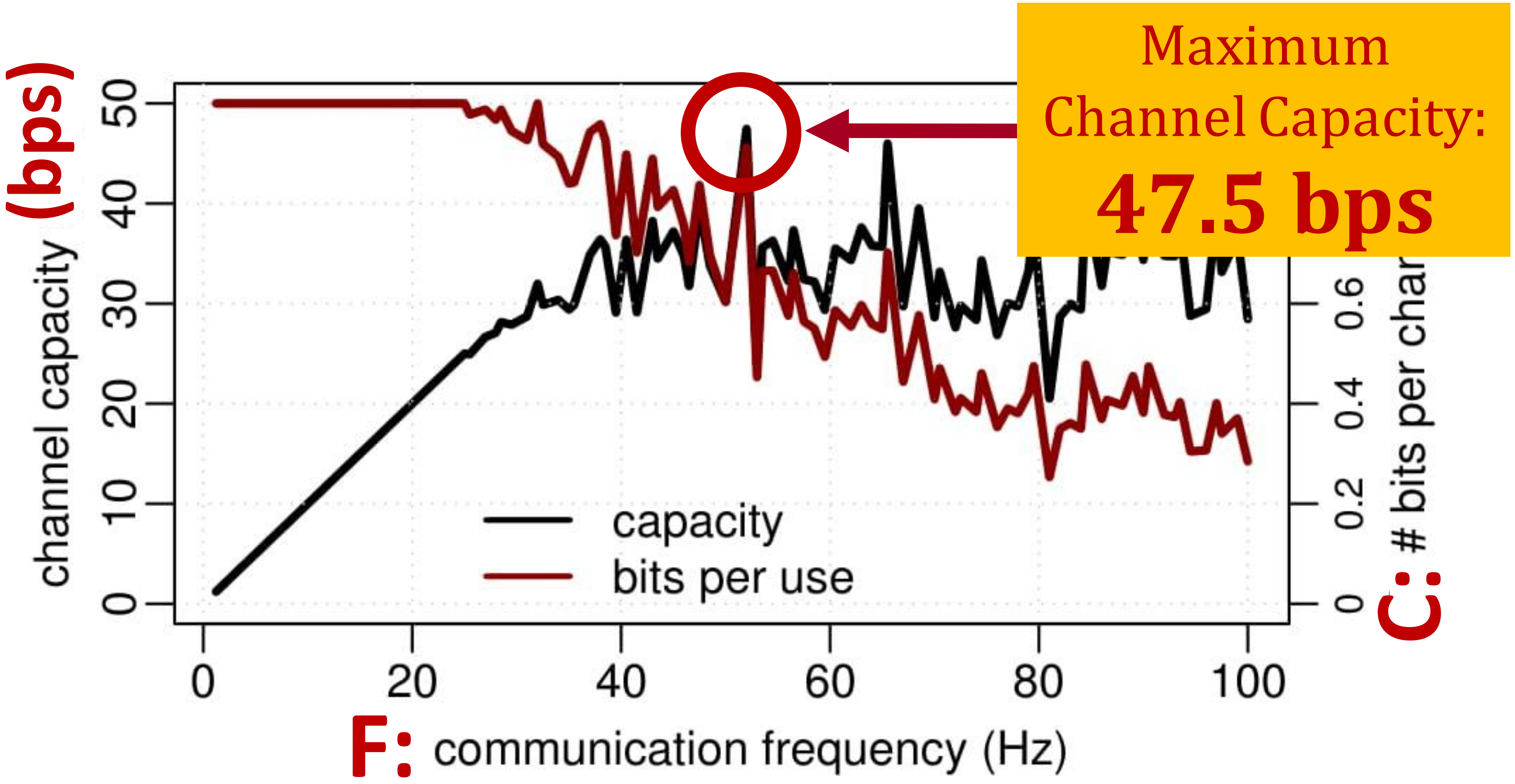


$C \approx 1$

Channel Capacity: Stronger Single-bit Encoding

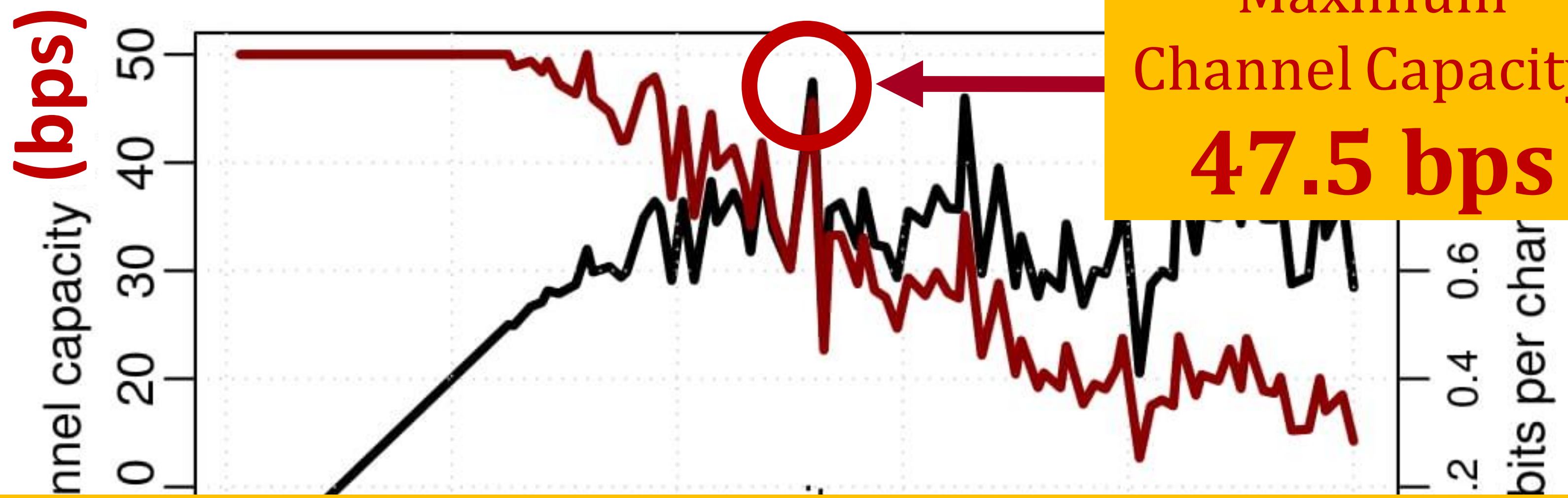


Channel Capacity: Stronger Single-bit Encoding



Maximum Channel Capacity: **47.5 bps**

Channel Capacity: Stronger Single-bit Encoding



Maximum Channel Capacity:
47.5 bps

POWERT channels enable **user data theft** at high rates, without needing any **privilege**.

Countermeasures?

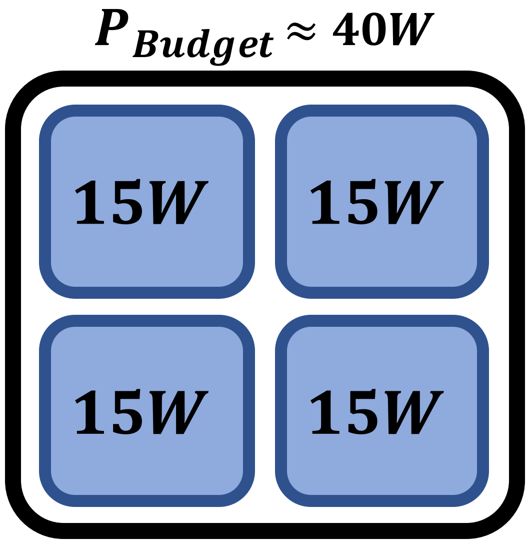
- ***Avoiding*** power budget sharing
- Operating frequency ***Randomization***
- ***Slowing down*** communication

Countermeasures?

- ***Avoiding*** power budget sharing
- Operating frequency ***Randomization***
- ***Slowing down*** communication

Avoiding Power Budget Sharing?

Avoiding Power Budget Sharing?

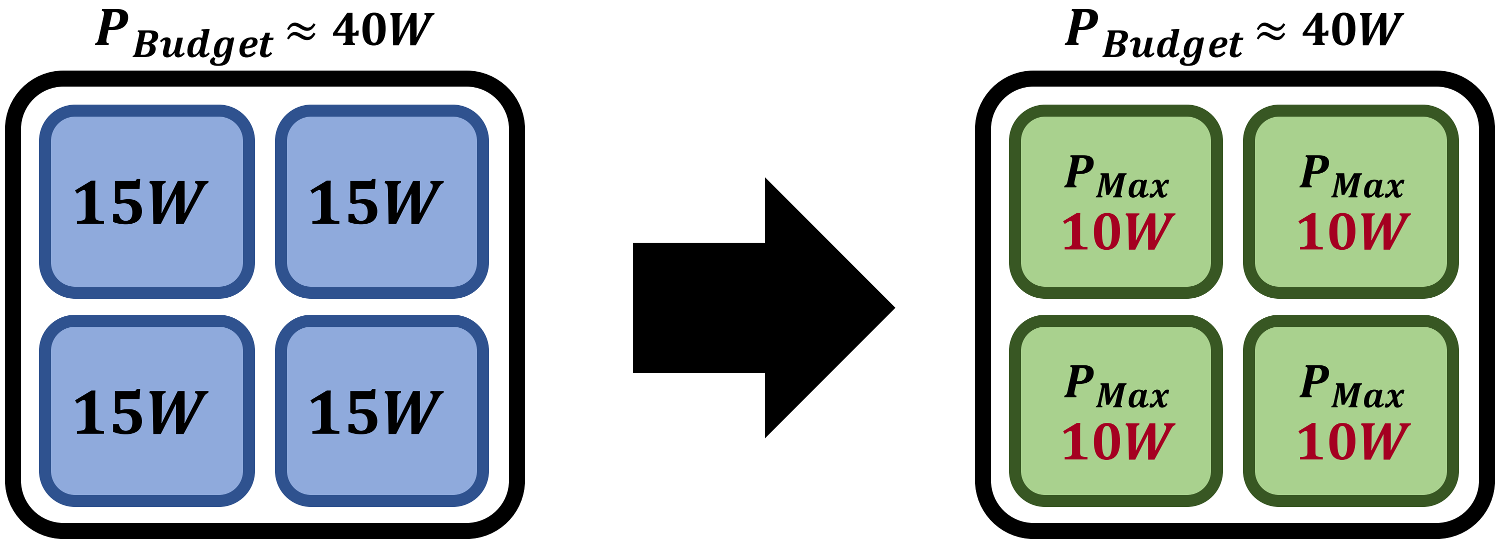


$P_{Budget} \approx 40W$

$15W$ $15W$

$15W$ $15W$

Avoiding Power Budget Sharing?



$P_{Budget} \approx 40W$

$15W$

$15W$

$15W$

$15W$

$P_{Budget} \approx 40W$

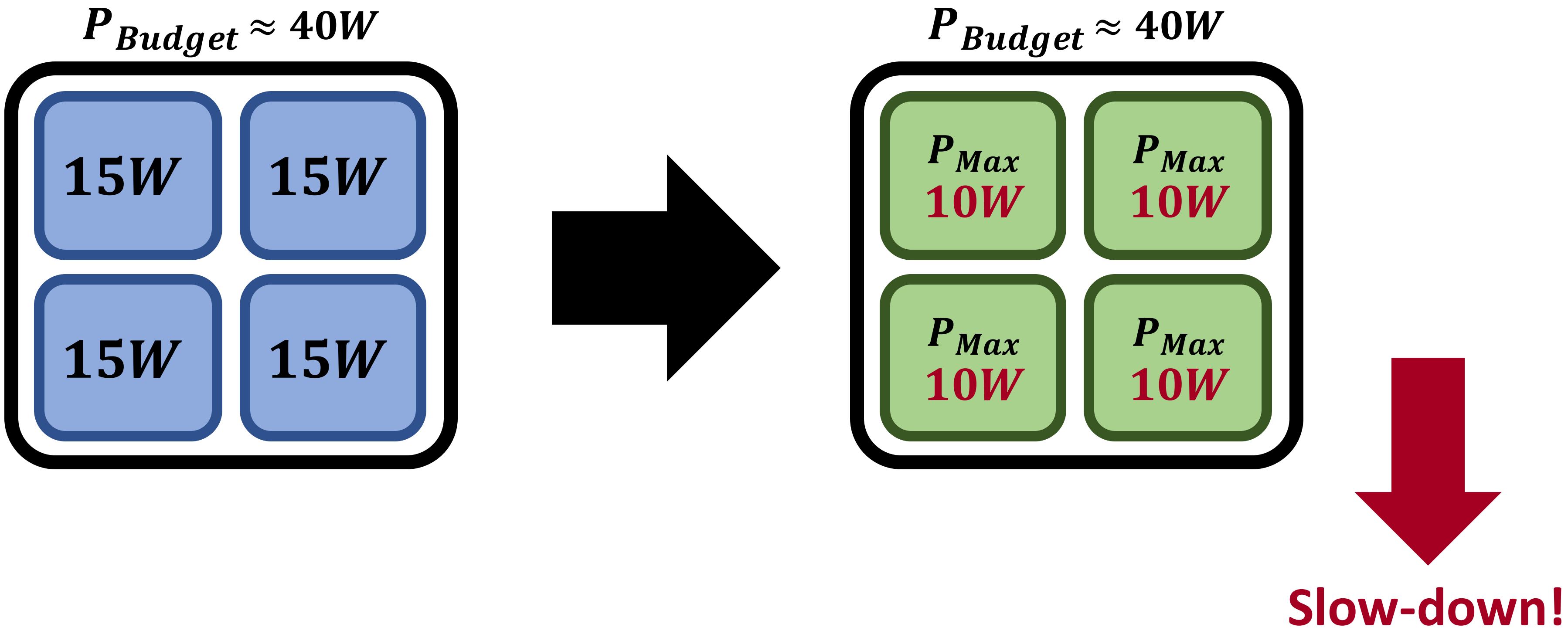
P_{Max} $10W$

P_{Max} $10W$

P_{Max} $10W$

P_{Max} $10W$

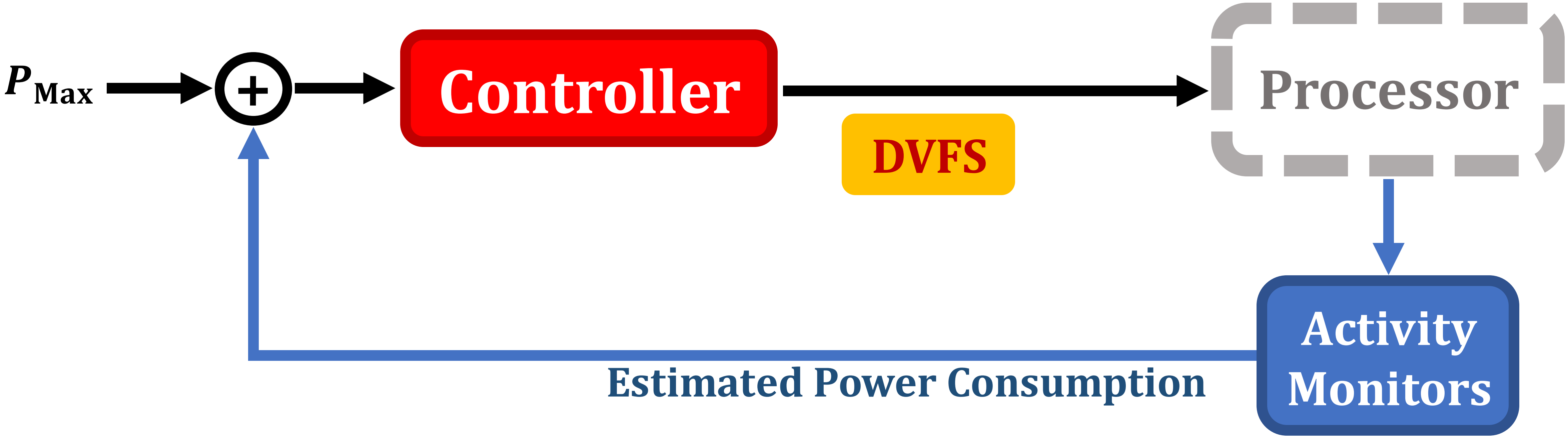
Avoiding Power Budget Sharing?



Countermeasures?

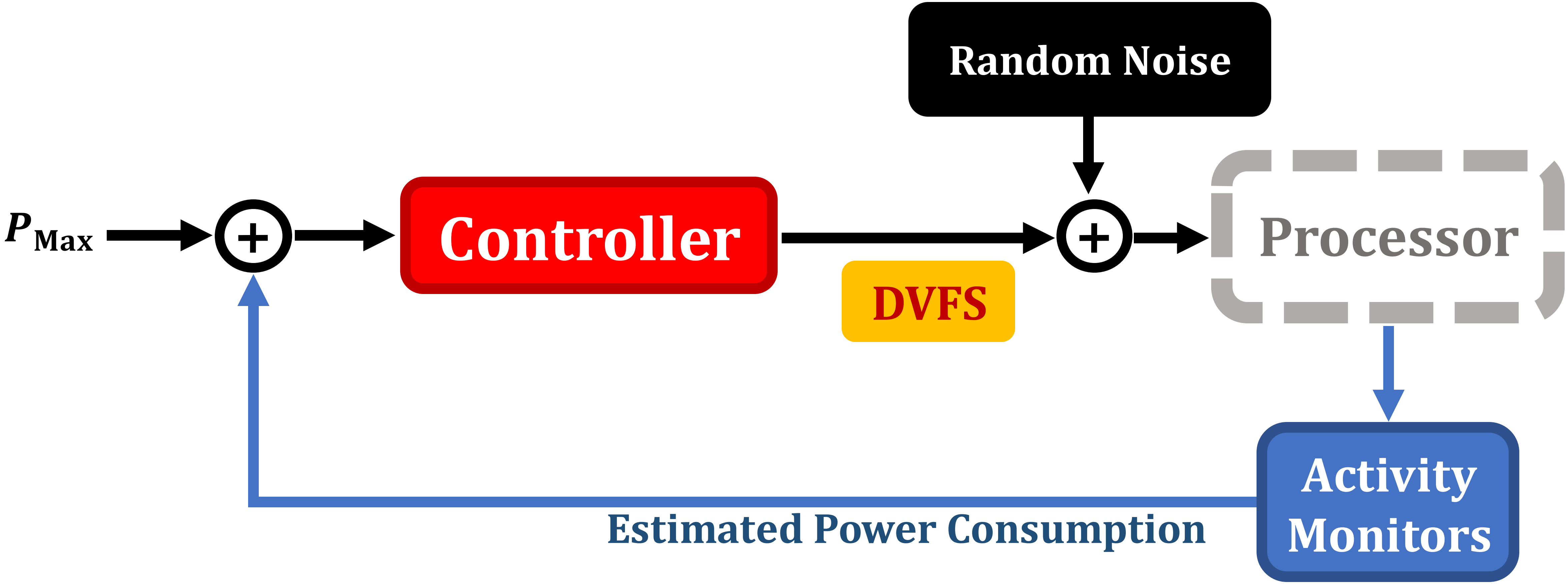
- ***Avoiding*** power budget sharing
- Operating frequency ***Randomization***
- ***Slowing down*** communication

Operating Frequency Randomization?



[P. Bose et. al., DATE, 2012.]

Operating Frequency Randomization?

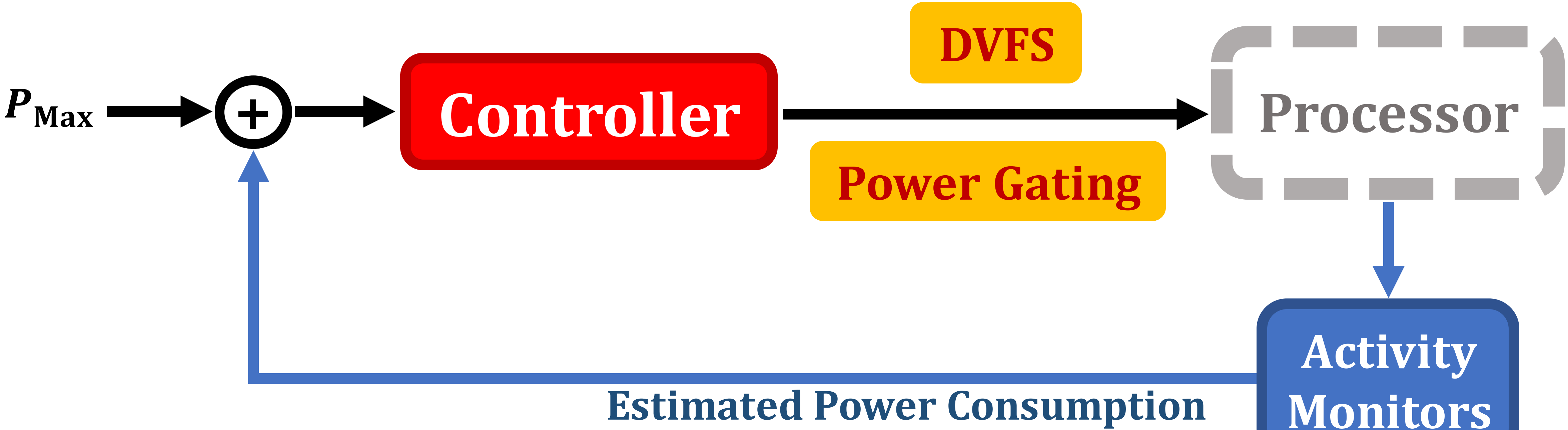


[P. Bose et. al., DATE, 2012.]

Countermeasures?

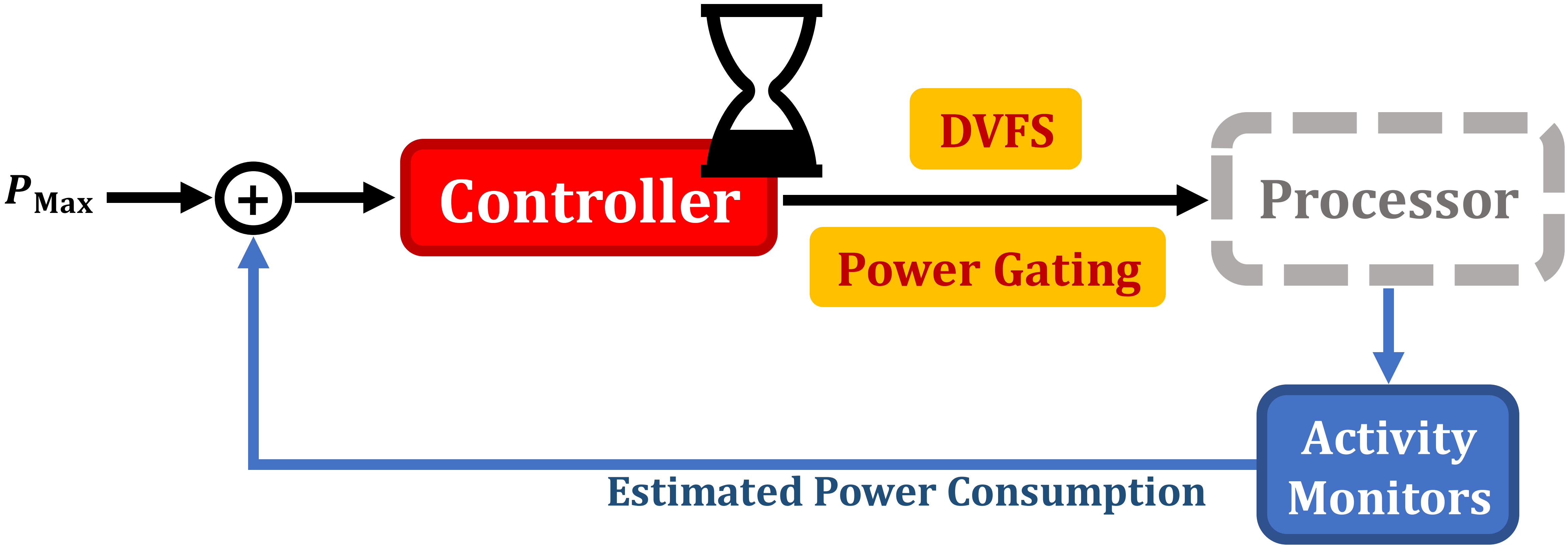
- ***Avoiding*** power budget sharing
- Operating frequency ***Randomization***
- ***Slowing down*** communication

Slowing Down Communication?



[P. Bose et. al., DATE, 2012.]

Slowing Down Communication?



[P. Bose et. al., DATE, 2012.]

Conclusion: POWERT Communication

- Enabled by power budget sharing

Conclusion: POWERT Communication

- Enabled by power budget sharing
- Generic, no privilege needed

Conclusion: POWERT Communication

- Enabled by power budget sharing
- Generic, no privilege needed
- Characterized on two representative platforms from industry
  - Observed a maximum channel capacity of **121.6 bps**

Conclusion: POWERT Communication

- Enabled by power budget sharing
- Generic, no privilege needed
- Characterized on two representative platforms from industry
  - Observed a maximum channel capacity of **121.6 bps**
  - Detailed **design space exploration**, **Sensitivity** study, and **platform-specific** analysis in the paper

Conclusion: POWERT Communication

- Enabled by power budget sharing
- Generic, no privilege needed
- Characterized on two representative platforms from industry
  - Observed a maximum channel capacity of **121.6 bps**
  - Detailed **design space exploration**, **Sensitivity** study, and **platform-specific** analysis in the paper
- Countermeasures?
  - Significant overheads on **performance** and/or **energy-efficiency**

Conclusion: POWERT Communication

- Enabled by power budget sharing
- Generic, no privilege needed
- Characterized on two representative platforms from industry
  - Observed a maximum channel capacity of **121.6 bps**
  - Detailed **design space exploration**, **Sensitivity** study, and **platform-specific** analysis in the paper
- Countermeasures?
  - Significant overheads on **performance** and/or **energy-efficiency**
  - More than 30% on evaluated platforms

POWERT Channels: A Novel Class of Covert Communication Exploiting Power Management Vulnerabilities

S. Karen Khatamifard, Longfei Wang, Amitabh Das, Selcuk Kose, Ulya R. Karpuzcu

UNIVERSITY OF MINNESOTA

USF UNIVERSITY OF SOUTH FLORIDA

UNIVERSITY of ROCHESTER