Ohm's Law in Data Centers:
A Voltage Side Channel for Timing Power Attacks

Mohammad A. Islam and **Shaolei Ren**

UC Riverside

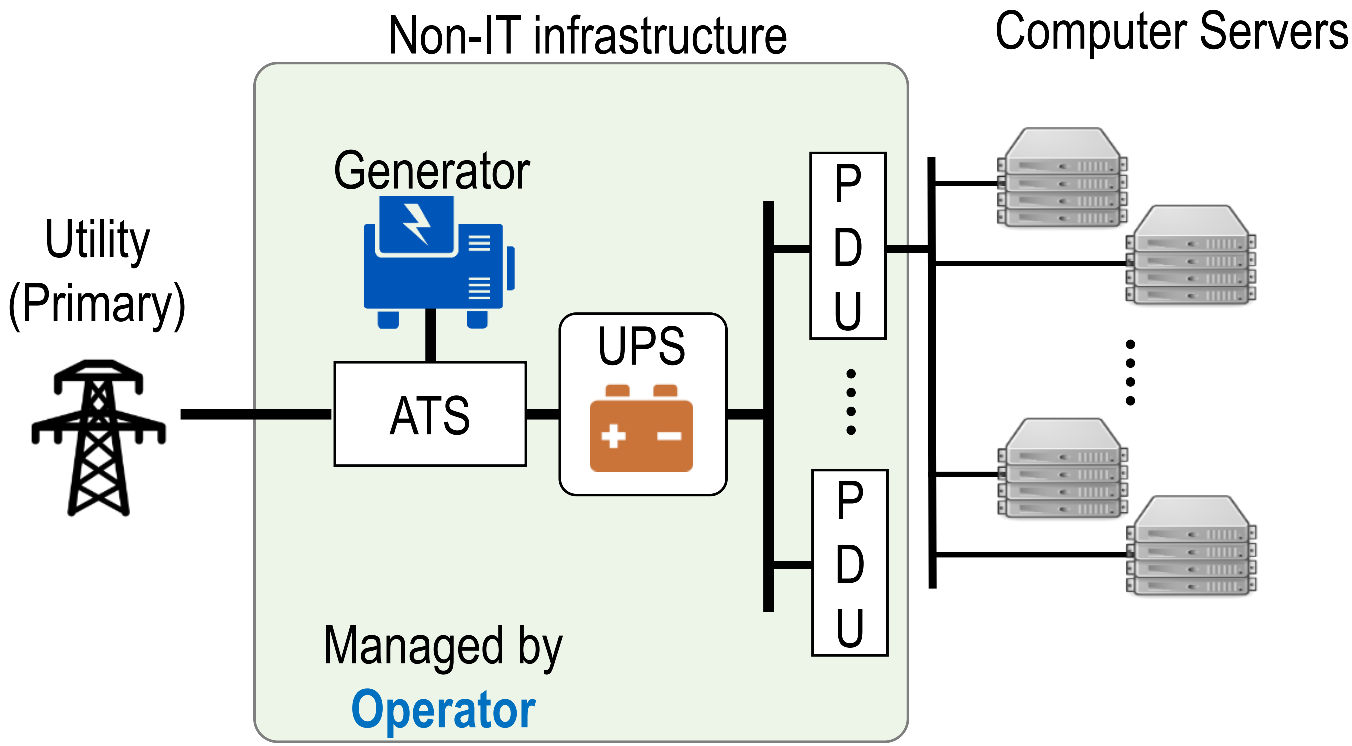
Acknowledgement: This work was supported in part by the U.S. NSF under grants CNS-1551661 and ECCS-1610471.

Cloud data centers

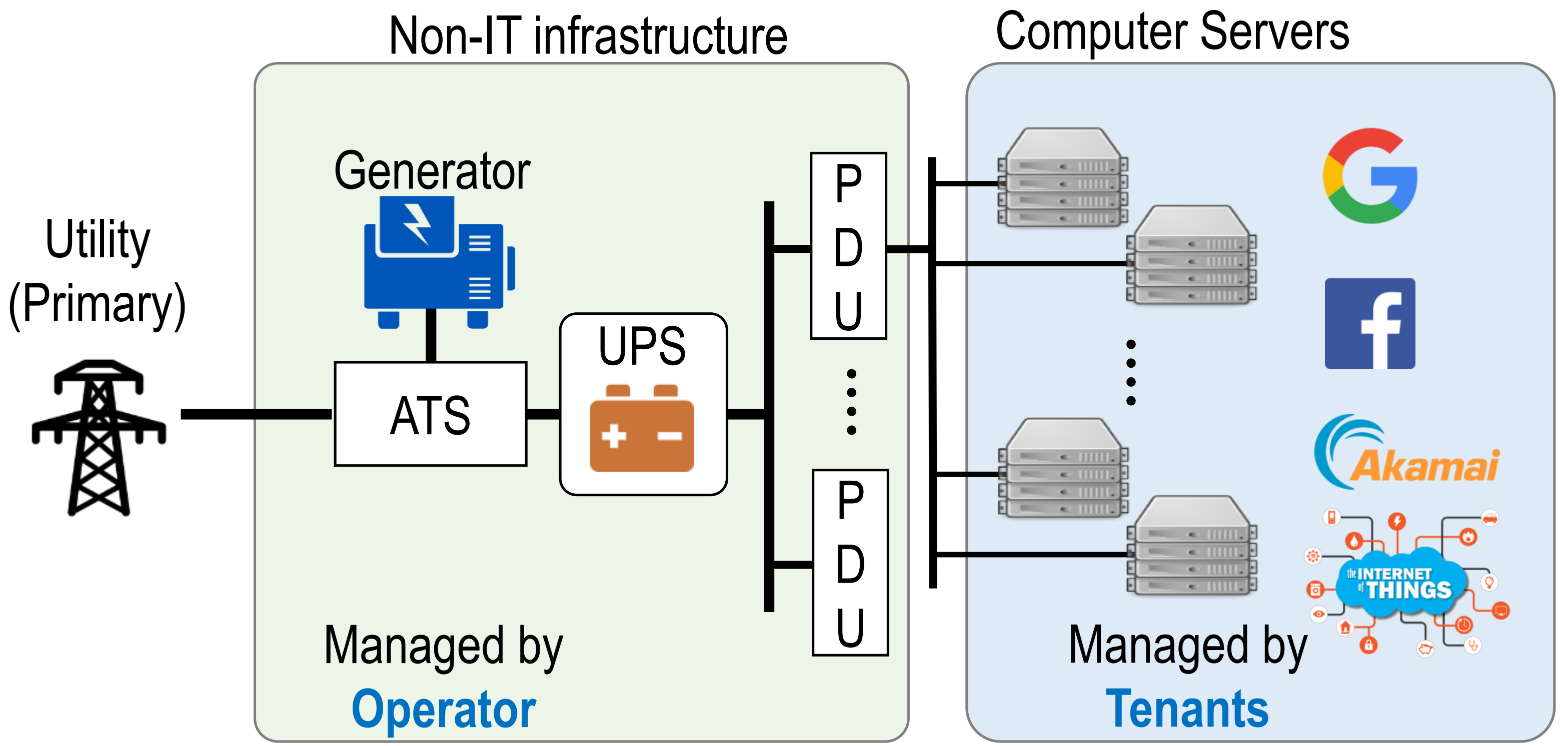
This talk is not about cloud data centers

User/Tenant = Virtual machines

Multi-tenant data centers (a.k.a. “colo”)



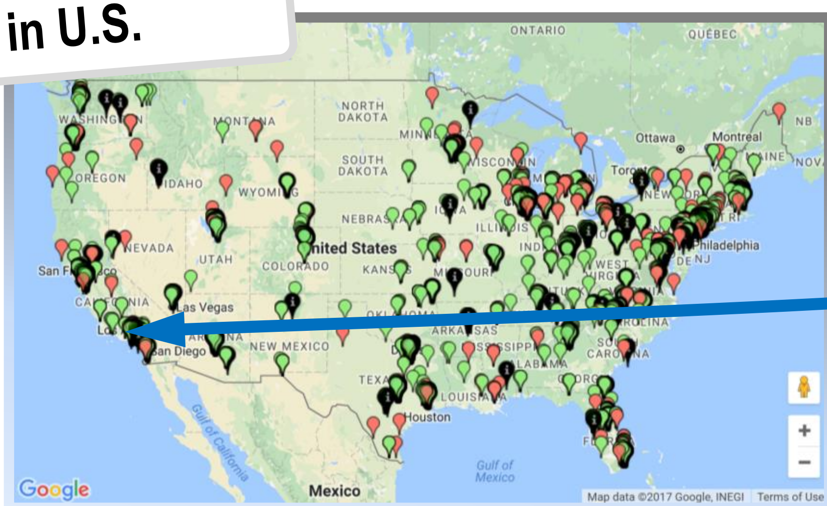
Multi-tenant data centers (a.k.a. “colo”)

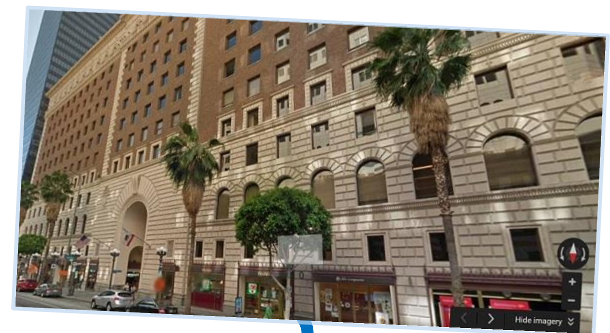


A shared data center facility that houses multiple tenants, each managing its own servers…

Multi-tenant data centers are everywhere…

2,000+ in U.S.

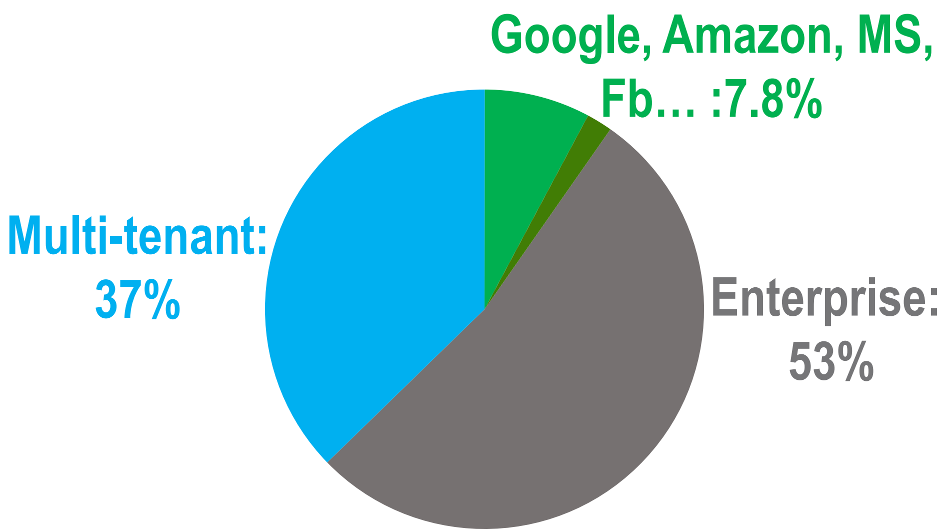




Apple houses 25% of its servers in multi-tenant data centers…

Multi-tenant data centers are everywhere…

2,000+



Percentage of electricity usage by data center type (source: NRDC 2015)

Apple houses 25% of its servers in multi-tenant data centers…

Data center security

- Mission-critical infrastructure
- Backbone of digital economy
- 50% growth by 2020
- IoT and edge computing
- ……

Securing the cyberspace is well studied

DDoS attack, network intrusion, privacy protection, etc.

[Mirkovic Sigcomm’04][Zhang CCS’12][Moon CCS’15][Dong CCS’17]…

Data center security

- Mission-critical infrastructure
- Backbone of digital economy
- 50% growth by 2020

Are the physical infrastructures secure?

- ……

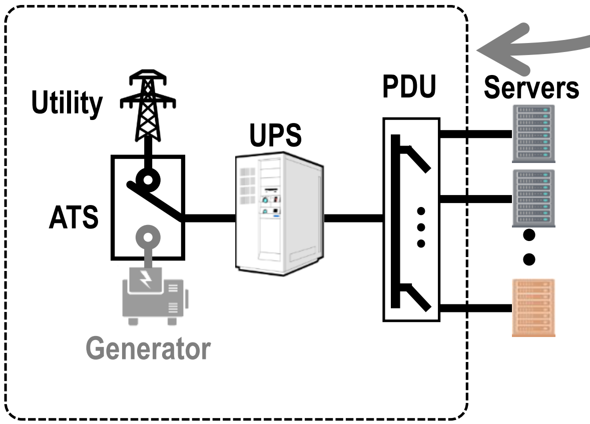
Securing the cyberspace is well studied

DDoS attack, network intrusion, privacy protection, etc.

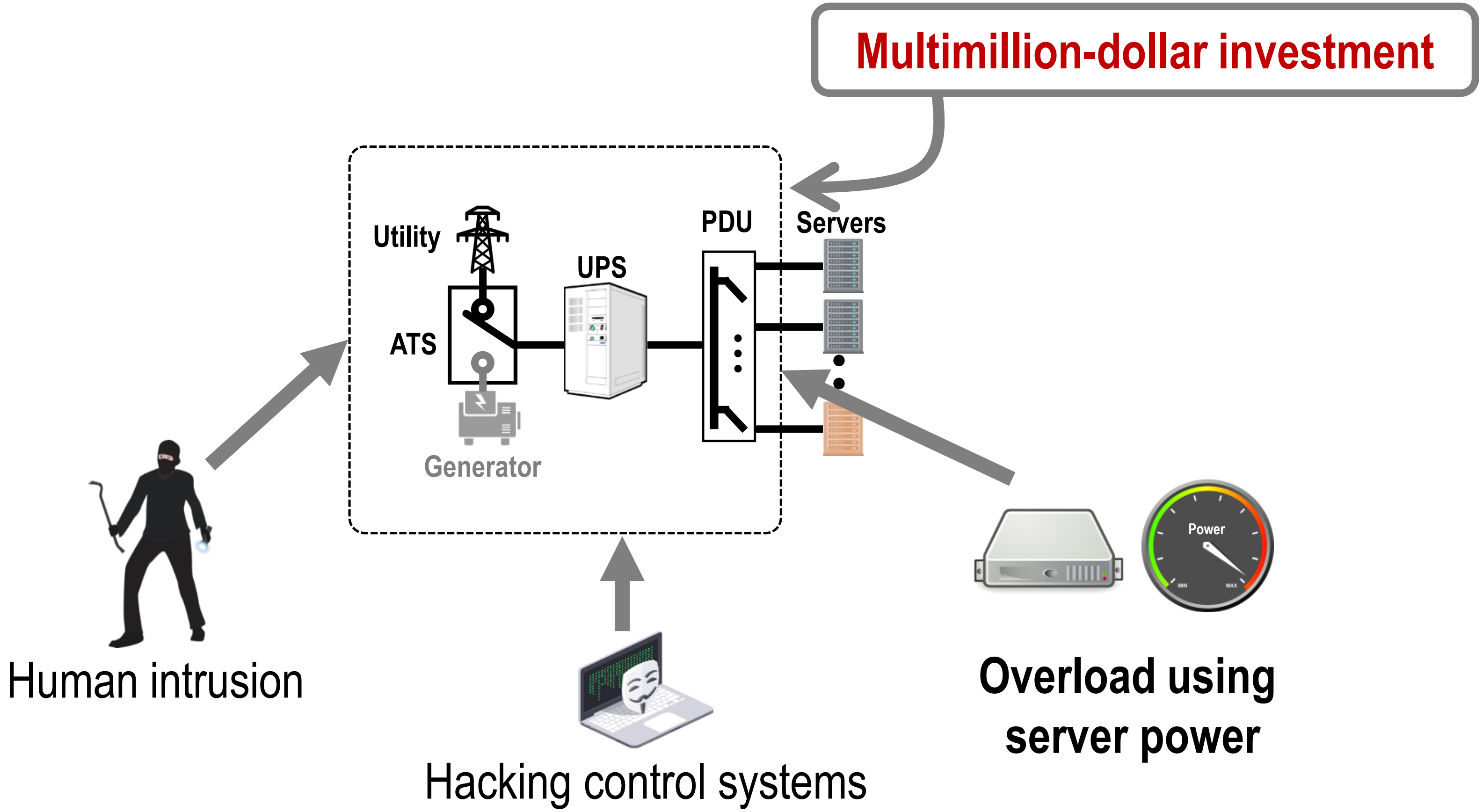
[Mirkovic Sigcomm'04][Zhang CCS'12][Moon CCS'15][Dong CCS'17]…

How to attack physical infrastructures?

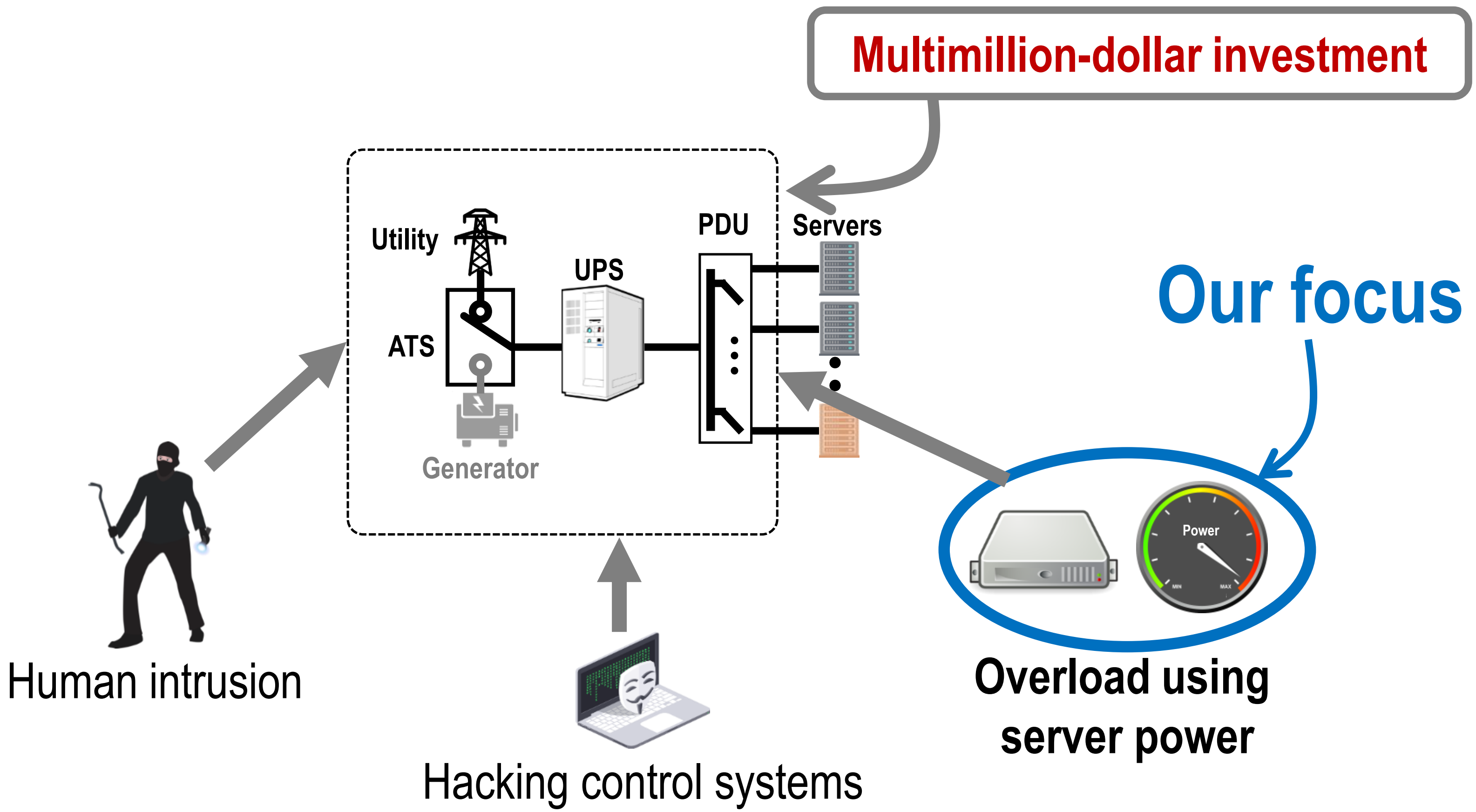
Multimillion-dollar investment



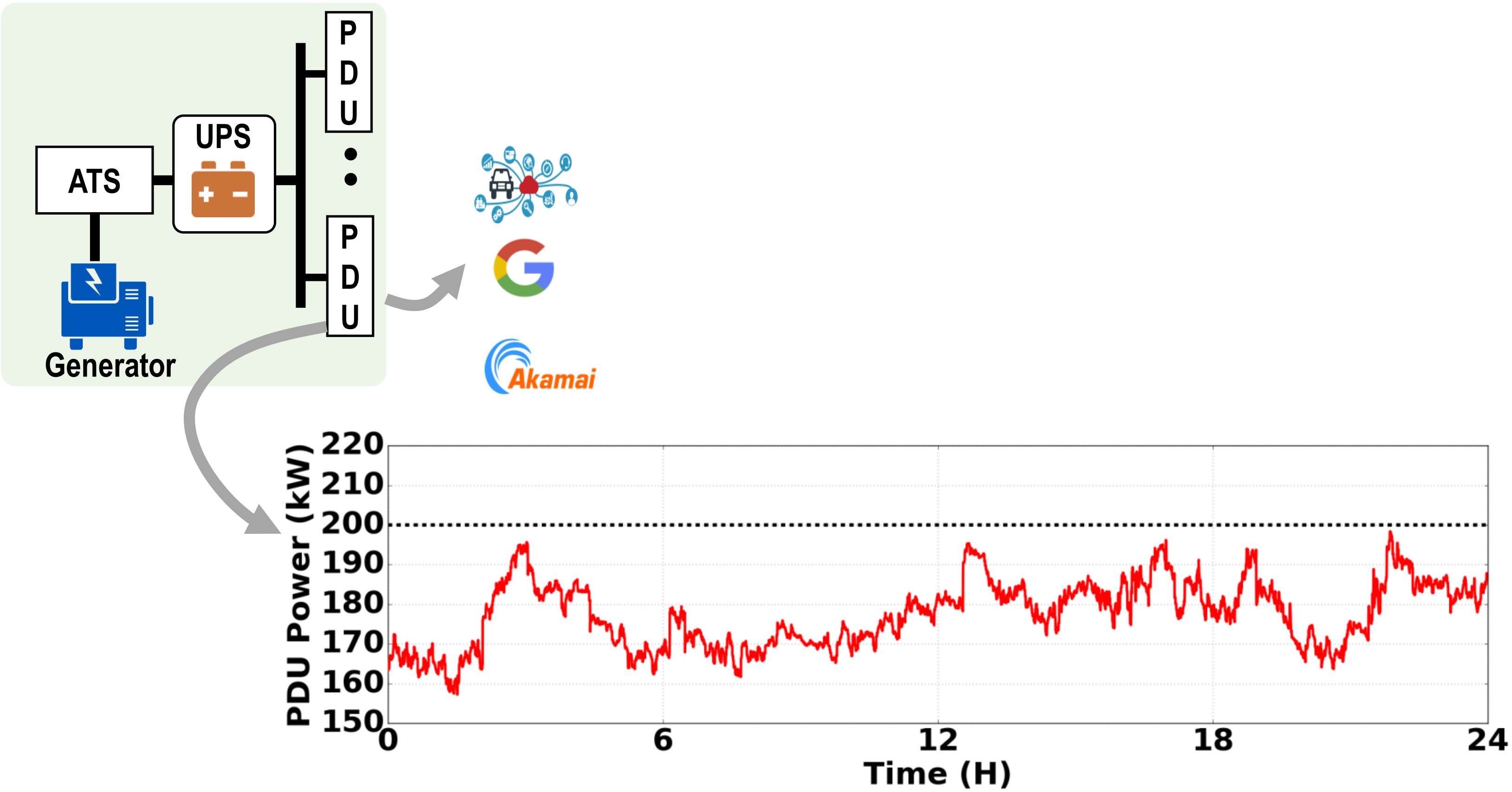
How to attack physical infrastructures?



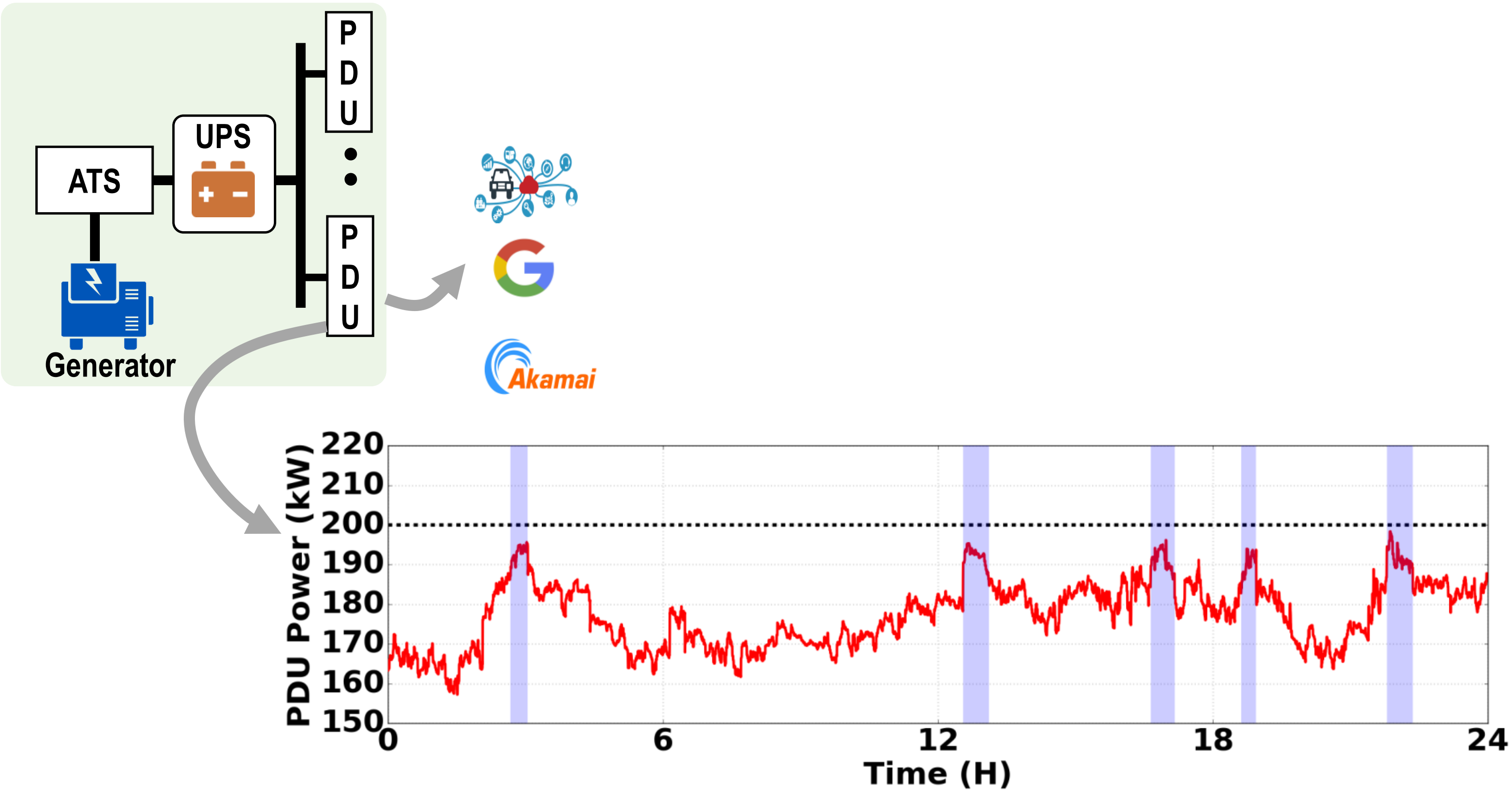
How to attack physical infrastructures?



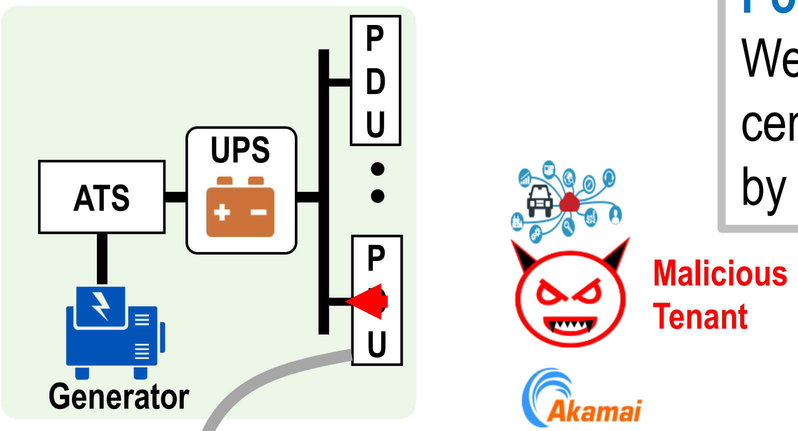
Threat model



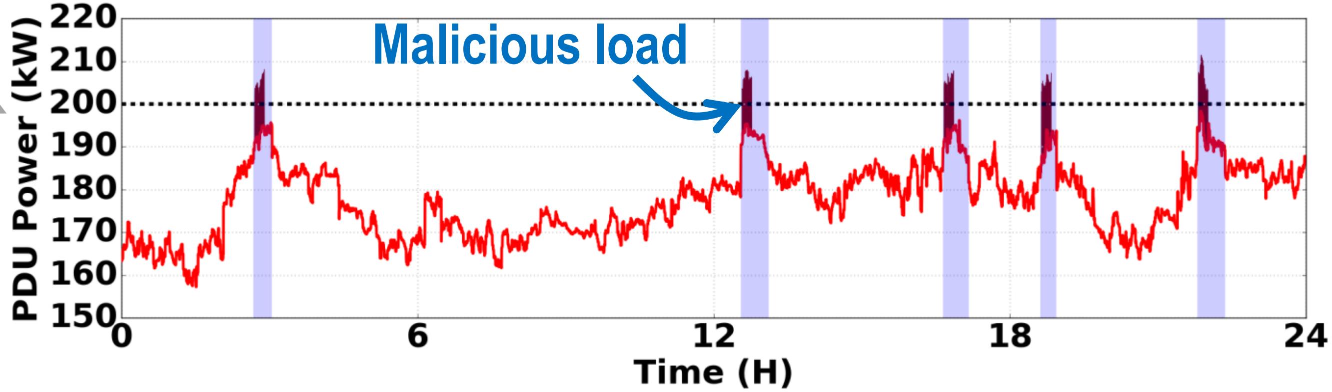
Threat model



Threat model



Power attack:
Well-timed power injection to overload the shared data center capacity, subject to all applicable constraints set by the operator

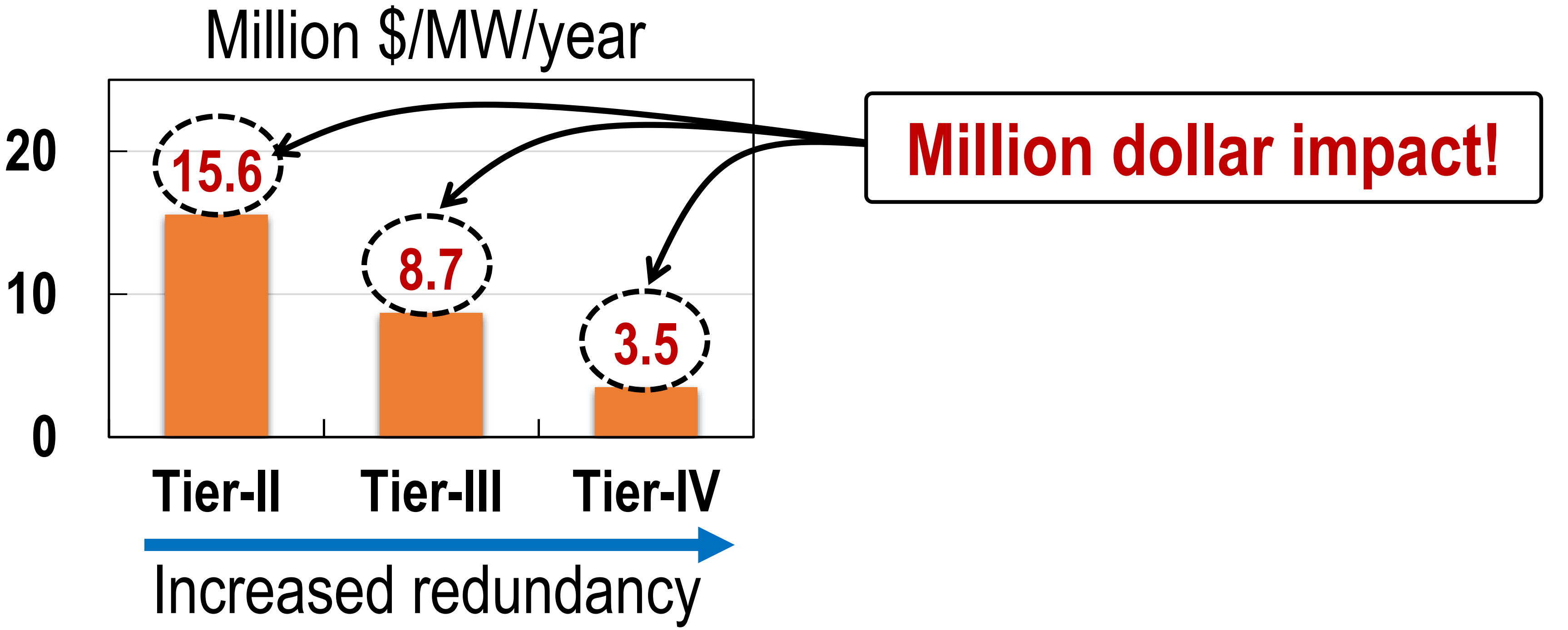


Threat model

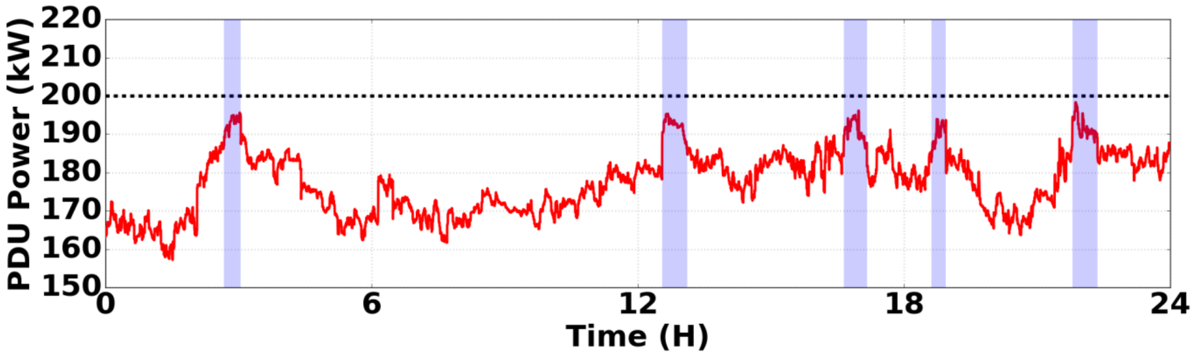
Power attacks make outages more likely
(~280x more likely for a Tier-IV data center)

Cost analysis of power attacks

Estimated impact of overloads (5% of the time, size: 1MW-10,00sqft)

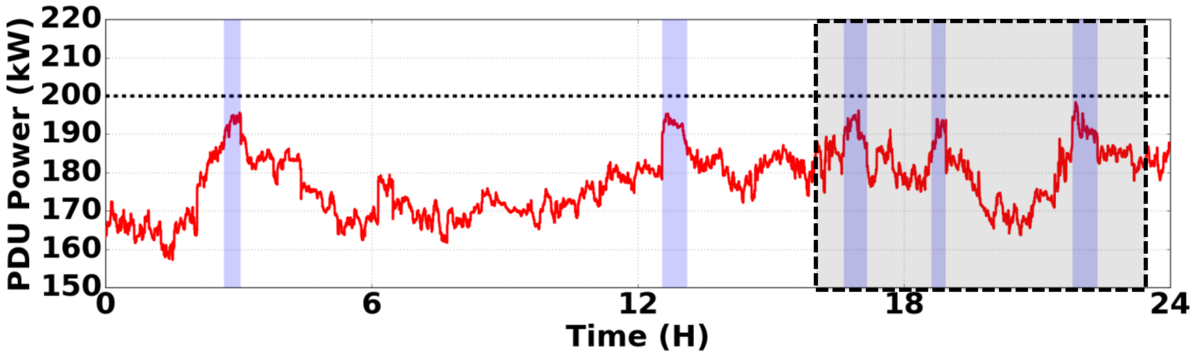


How to precisely time power attacks?



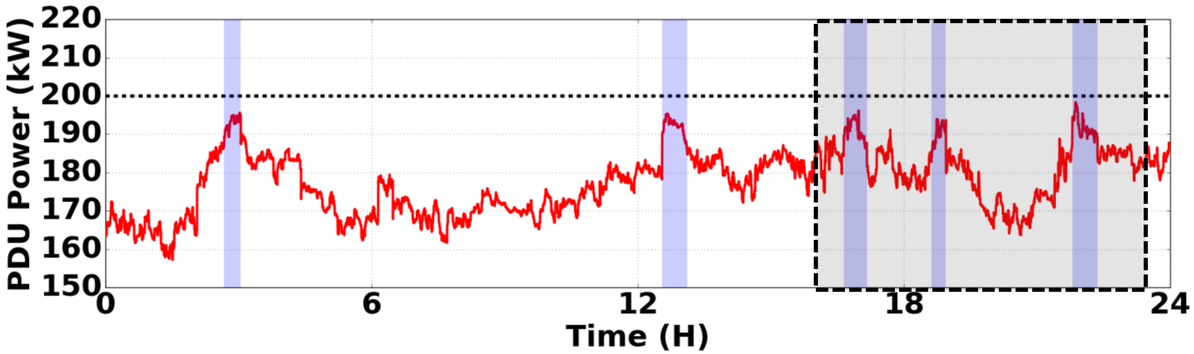
- Random attacks are unlikely to be successful, while constant full power is prohibited

How to precisely time power attacks?



- Random attacks are unlikely to be successful, while constant full power is prohibited
- Coarse timing (e.g., based on “peak” hours) is ineffective

How to precisely time power attacks?



- Random attacks are unlikely to be successful, while constant full power is prohibited
- Coarse timing (e.g., based on “peak” hours) is ineffective

How to estimate the power load without power meters?

“Wireless” side channels

Thermal: Higher power produces more heat

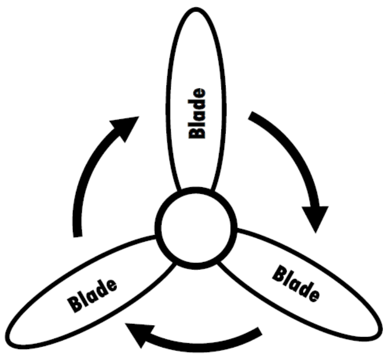
- Requires heat recirculation model
- Slow responses
- Only applicable to raised-floor designs

References

- M. A. Islam, **S. Ren**, and A. Wierman, “Exploiting a Thermal Side Channel for Power Attacks in Multi-Tenant Data Centers,” ACM Conference on Computer and Communications Security (**CCS**), 2017.
- M. A. Islam, L. Yang, K. Ranganath, and **S. Ren**, “Why Some Like It Loud: Timing Power Attacks in Multi-tenant Data Centers Using an Acoustic Side Channel,” ACM International Conference on Measurement and Modeling of Computer Systems (**SIGMETRICS**), 2018.

"Wireless" side channels

Thermal: Higher power produces more heat
- Requires heat recirculation model
- Slow responses
- Only applicable to raised-floor designs



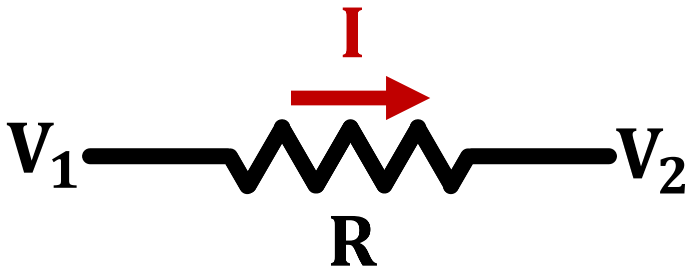
Acoustic: More heat requires more cold air
- Inaccurate timing due to near-far effects
- Limited distance
- Easy to degrade by injecting additional noise

References

- M. A. Islam, **S. Ren**, and A. Wierman, "Exploiting a Thermal Side Channel for Power Attacks in Multi-Tenant Data Centers," ACM Conference on Computer and Communications Security (**CCS**), 2017.
- M. A. Islam, L. Yang, K. Ranganath, and **S. Ren**, "Why Some Like It Loud: Timing Power Attacks in Multi-tenant Data Centers Using an Acoustic Side Channel," ACM International Conference on Measurement and Modeling of Computer Systems (**SIGMETRICS**), 2018.

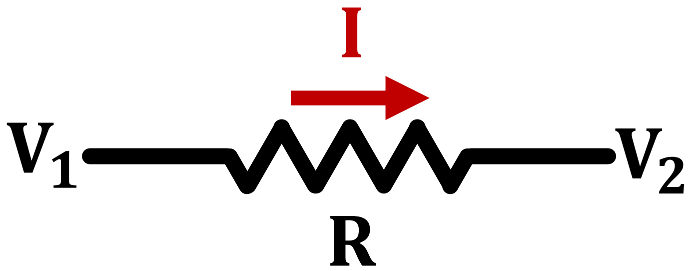
A voltage side channel due to Ohm’s Law

Ohm’s Law



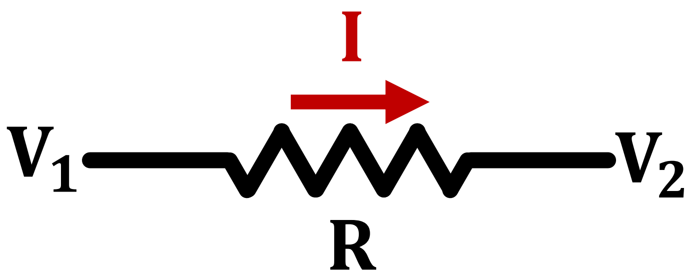
$$\mathbf{V} = \mathbf{I} \cdot \boldsymbol{R}$$

Ohm's Law



$$\mathbf{V_1} - \mathbf{V_2} = \mathbf{I} \cdot \boldsymbol{R}$$

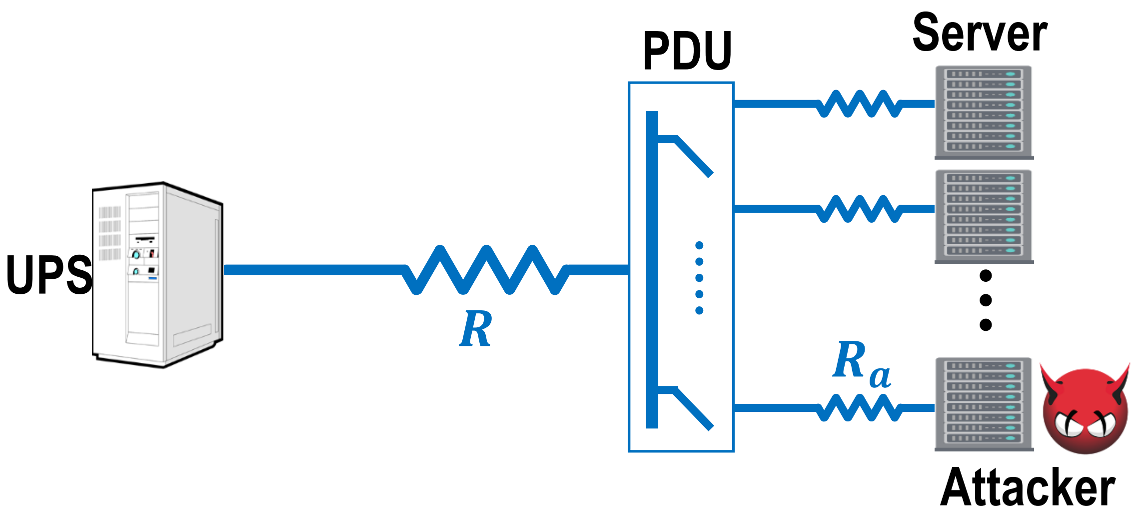
Ohm’s Law



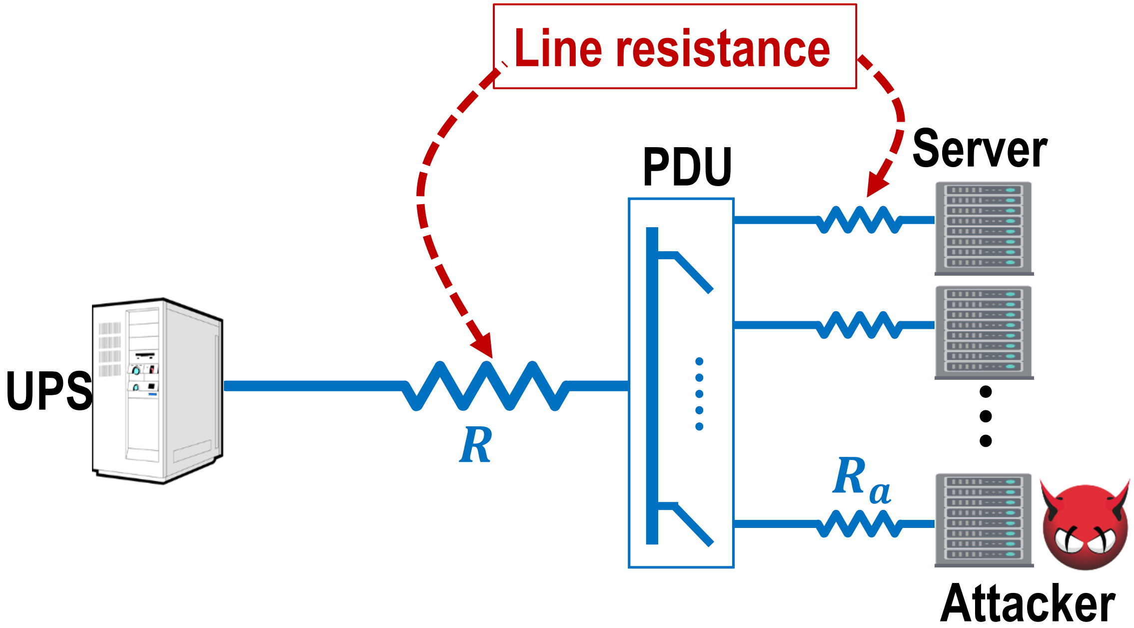
$$\boxed{\mathbf{V_2}} = \mathbf{V_1} - \boxed{\mathbf{I}} \cdot \boldsymbol{R}$$

The voltage at the other end depends on the current

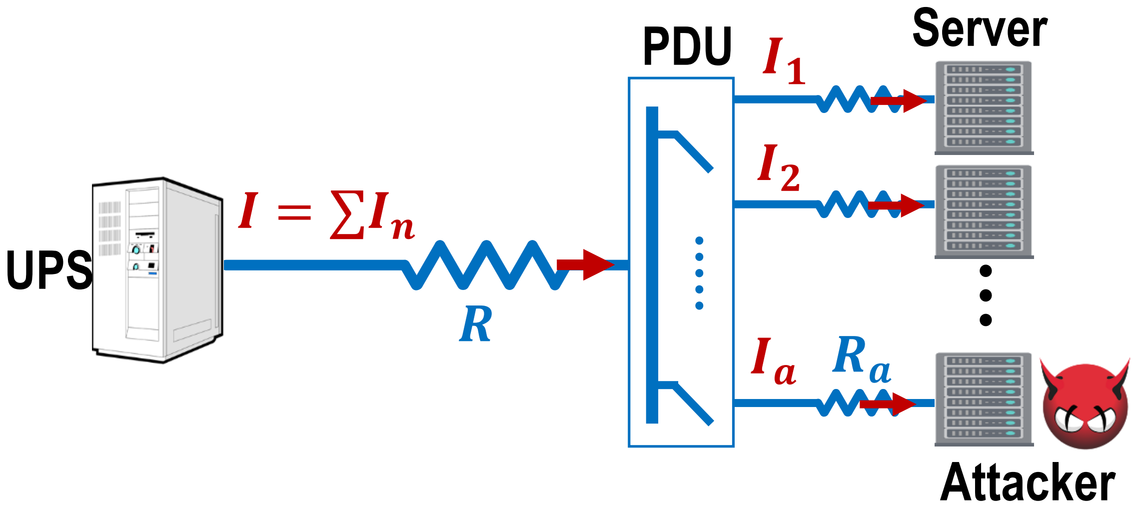
Ohm's Law in data centers



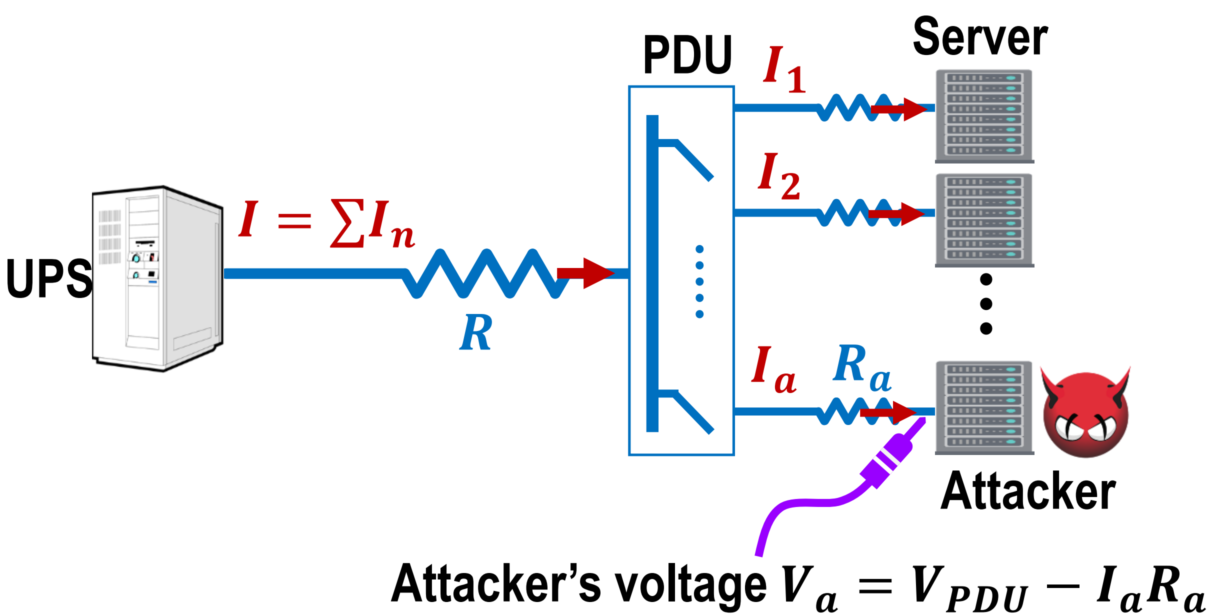
Ohm’s Law in data centers

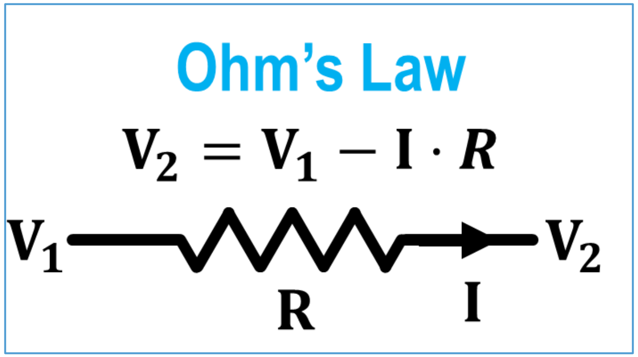


Ohm’s Law in data centers

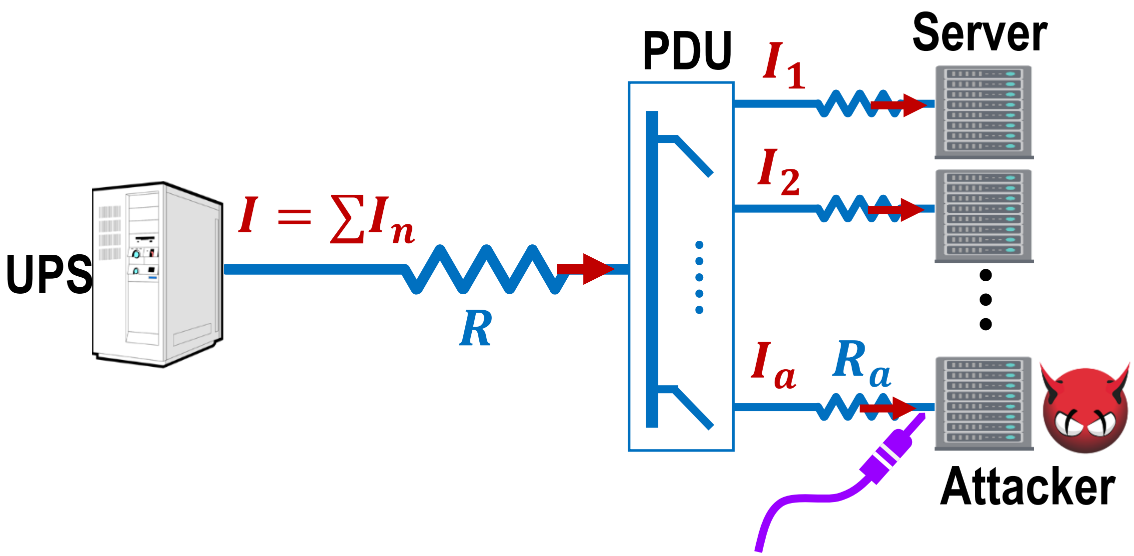


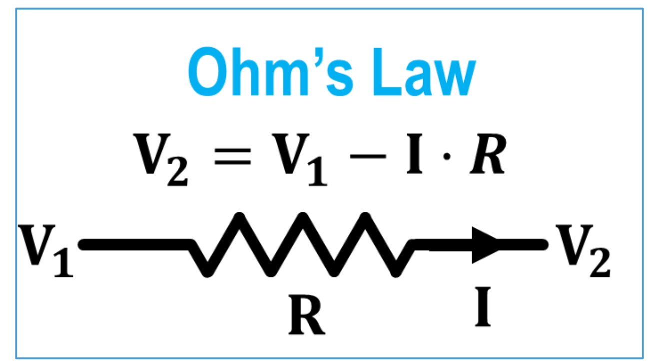
Ohm's Law in data centers





Ohm’s Law in data centers





Attacker’s voltage $V_a = V_{PDU} - I_a R_a$

$$= \overbrace{V_{UPS} - \boxed{\sum I_n R}} - \boxed{I_a R_a}$$

Power load is included in V_a

Own impact

A voltage side channel

Attacker's voltage $V_a = V_{UPS} - \boxed{\sum I_n R} - I_a R_a$

A voltage side channel

ΔV based attack:

Low voltage → High current/load→ Attack opportunity?

Attacker's voltage $V_a = V_{UPS} - \boxed{\sum I_n R} - I_a R_a$

A voltage side channel

ΔV based attack:

Low voltage → High current/load→ Attack opportunity?

Attacker's voltage $V_a = \boxed{V_{UPS}} - \boxed{\sum I_n R} - I_a R_a$

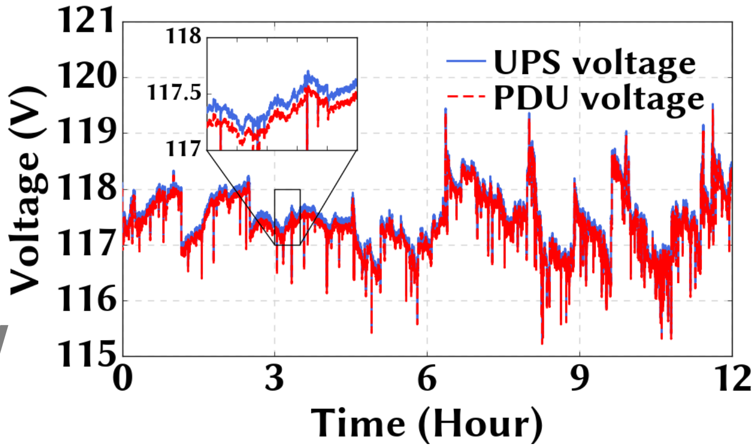
Large random variation from power grid

A voltage side channel

ΔV based attack:
Low voltage → High current/load→ Attack opportunity?

Attacker's voltage $V_a = \boxed{V_{UPS}} - \boxed{\sum I_n R} - I_a R_a$

Large random variation
from power grid



- Grid variation = ~3V
- Voltage drop variation = ~10mV

A voltage side channel

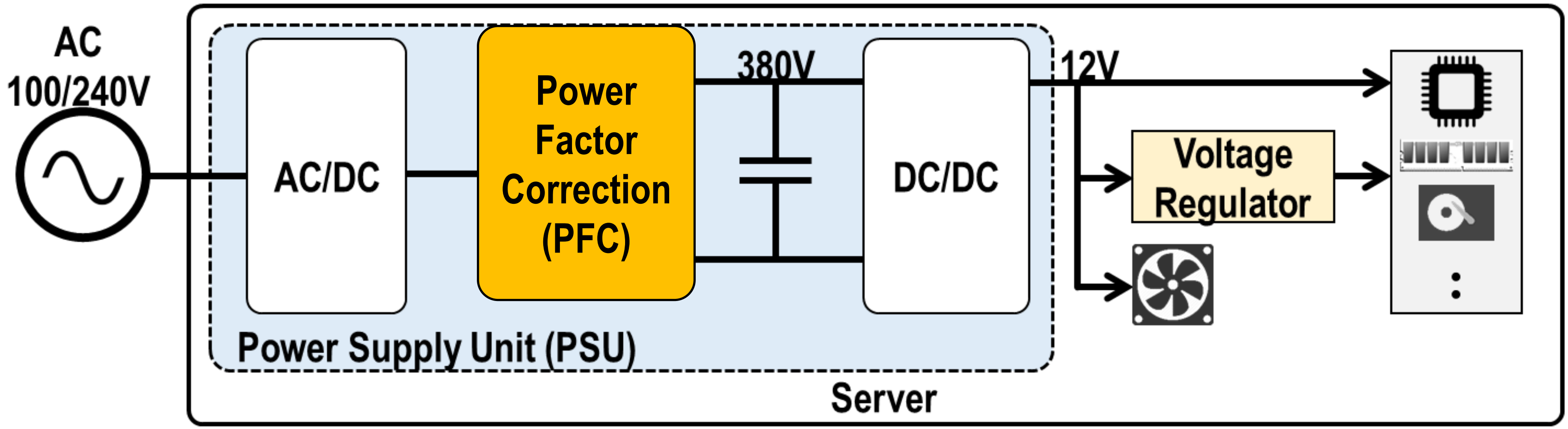
ΔV based attack:
Low voltage → High current/load → Attack opportunity?

How to extract power load information from voltage signals?

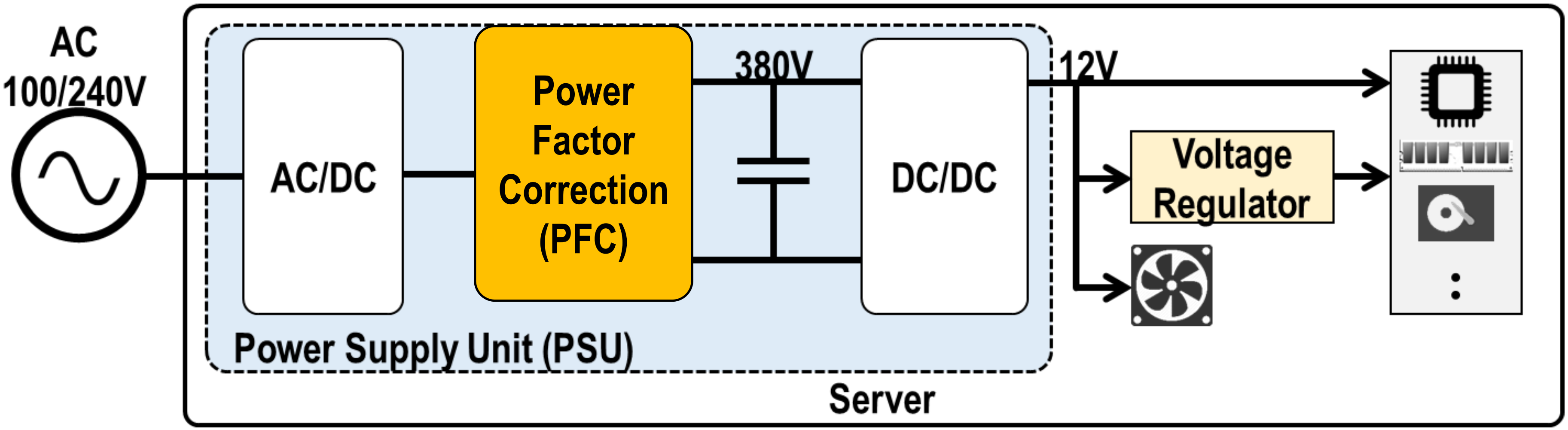
Large random variation from power grid

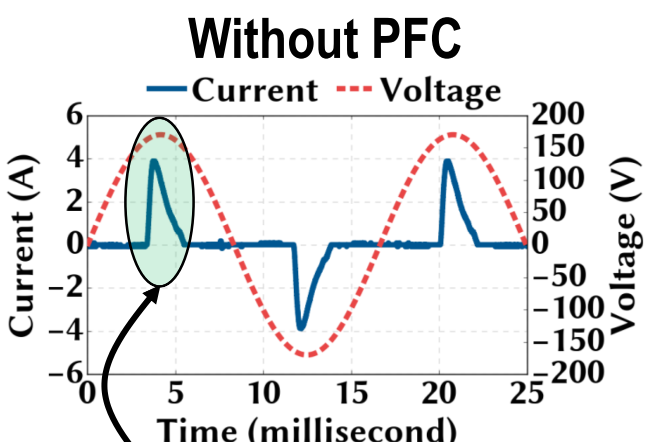
- Grid variation = ~3V
- Voltage drop variation = ~10mV

A closer look at server's power supply



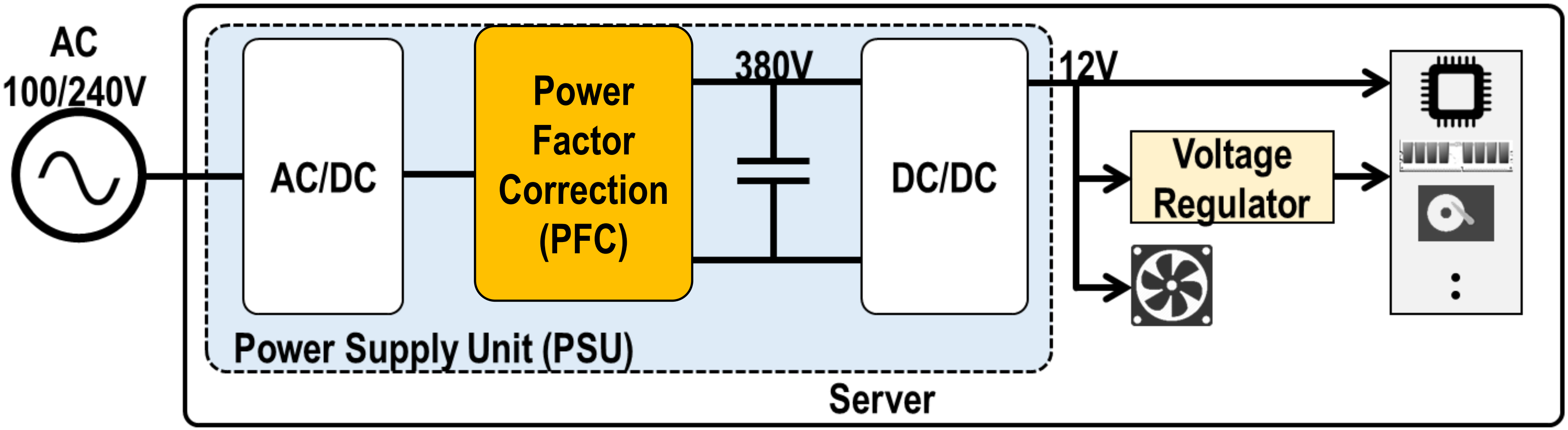
A closer look at server's power supply

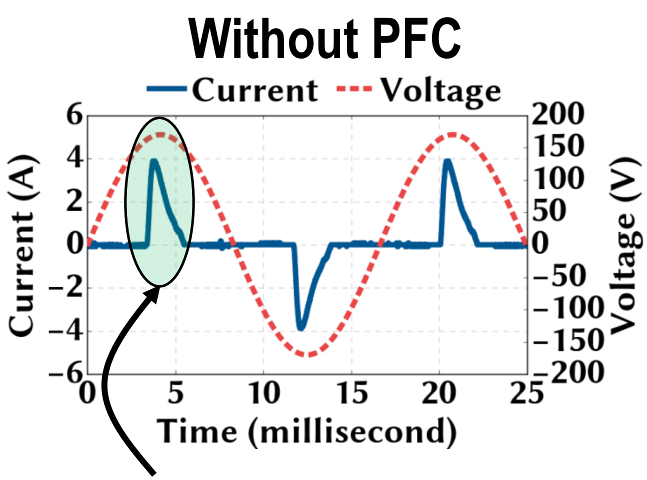




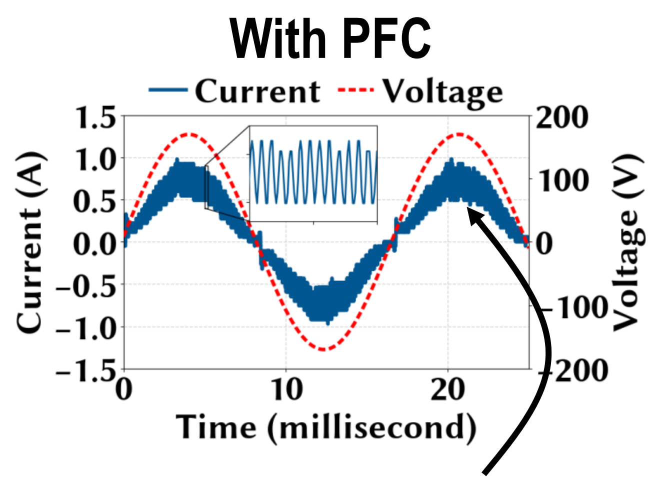
Current draw is bursty

A closer look at server’s power supply



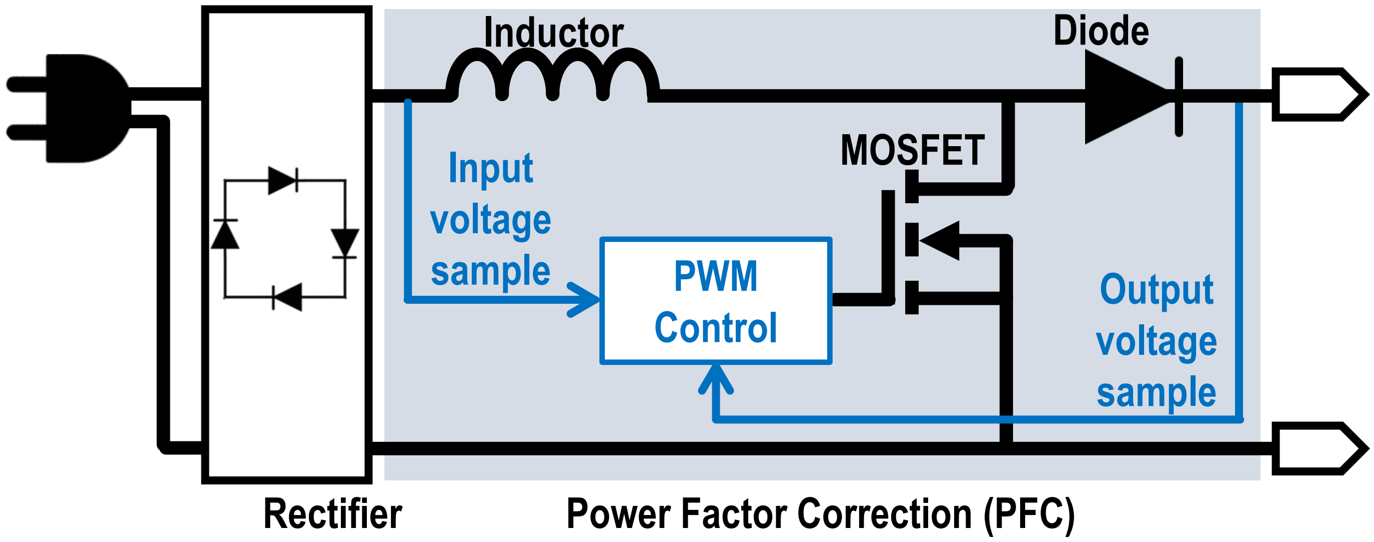


Current draw is bursty

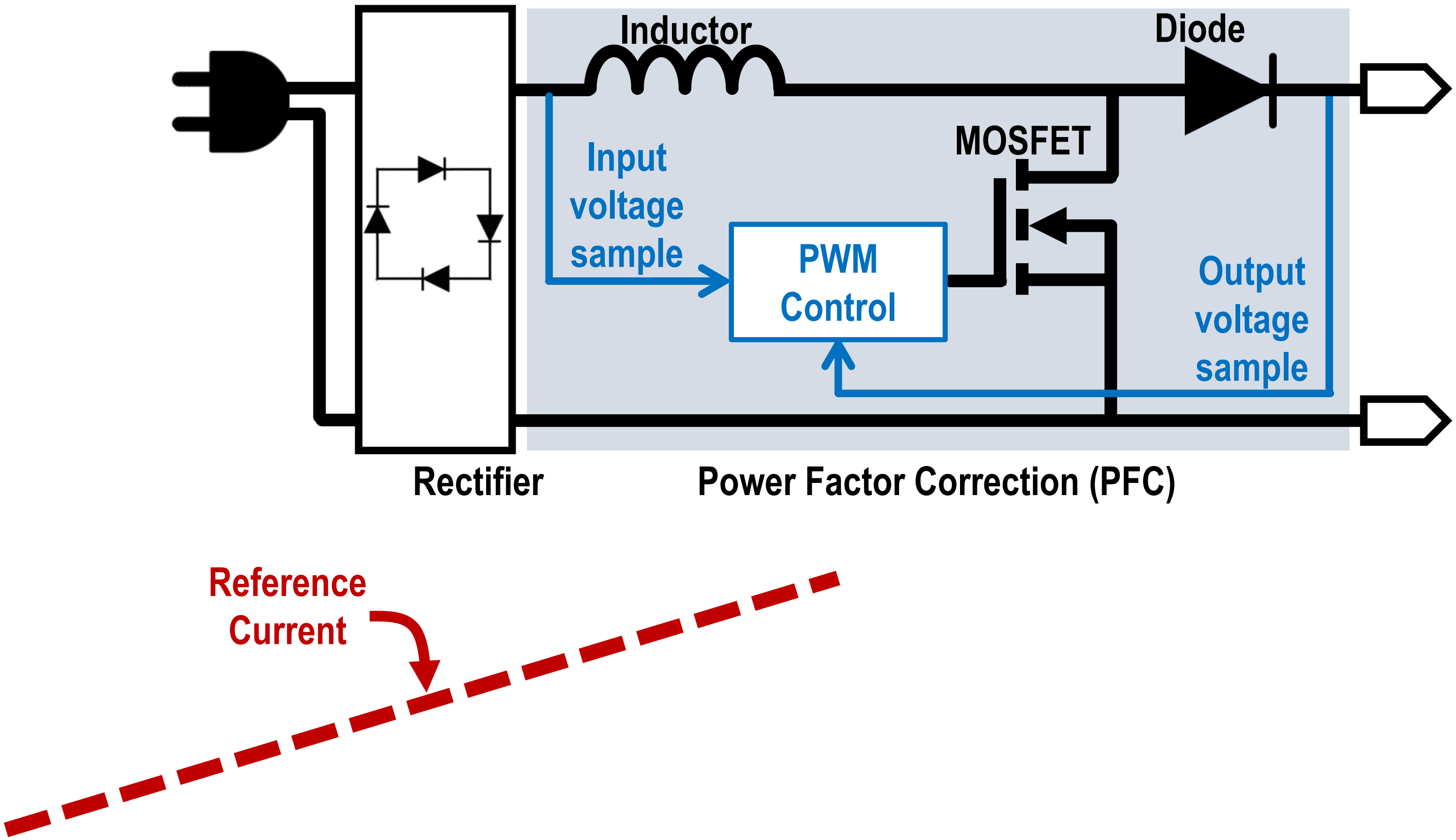


Current follows a sinewave with **high-frequency ripples**

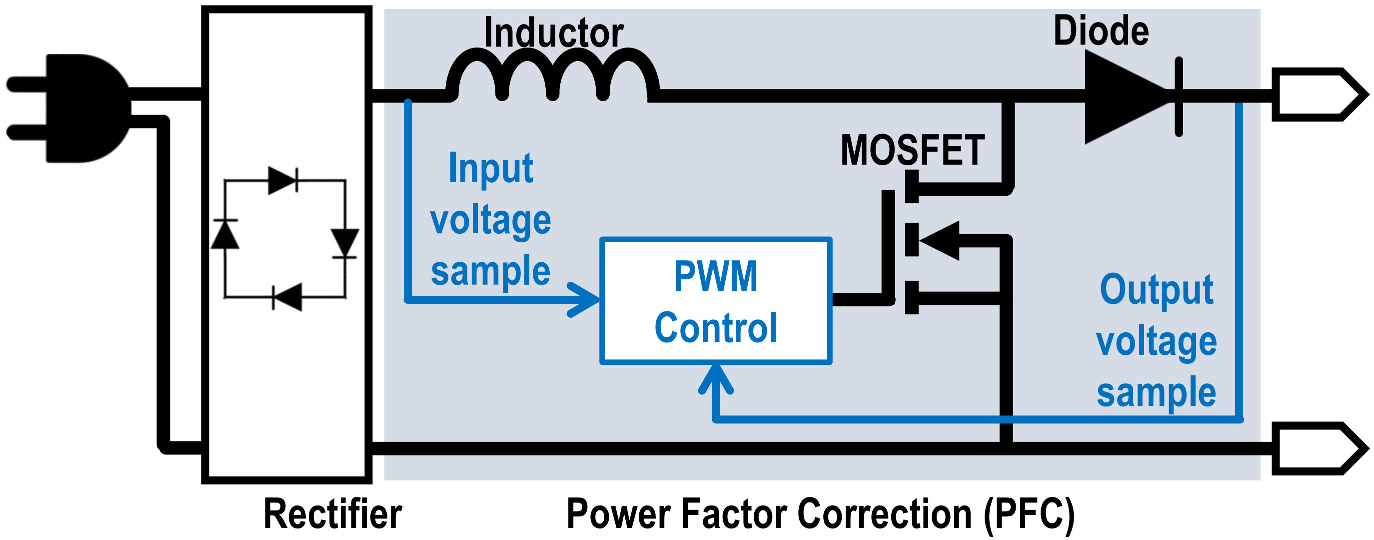
The ripples come from the PFC control

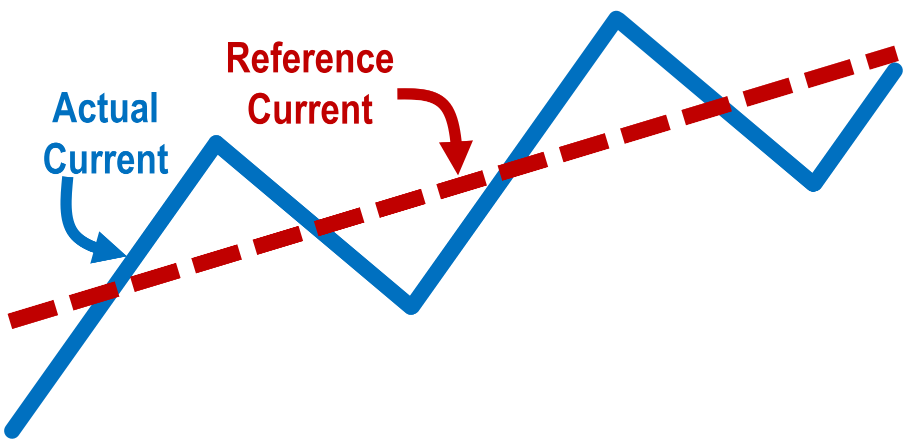


The ripples come from the PFC control

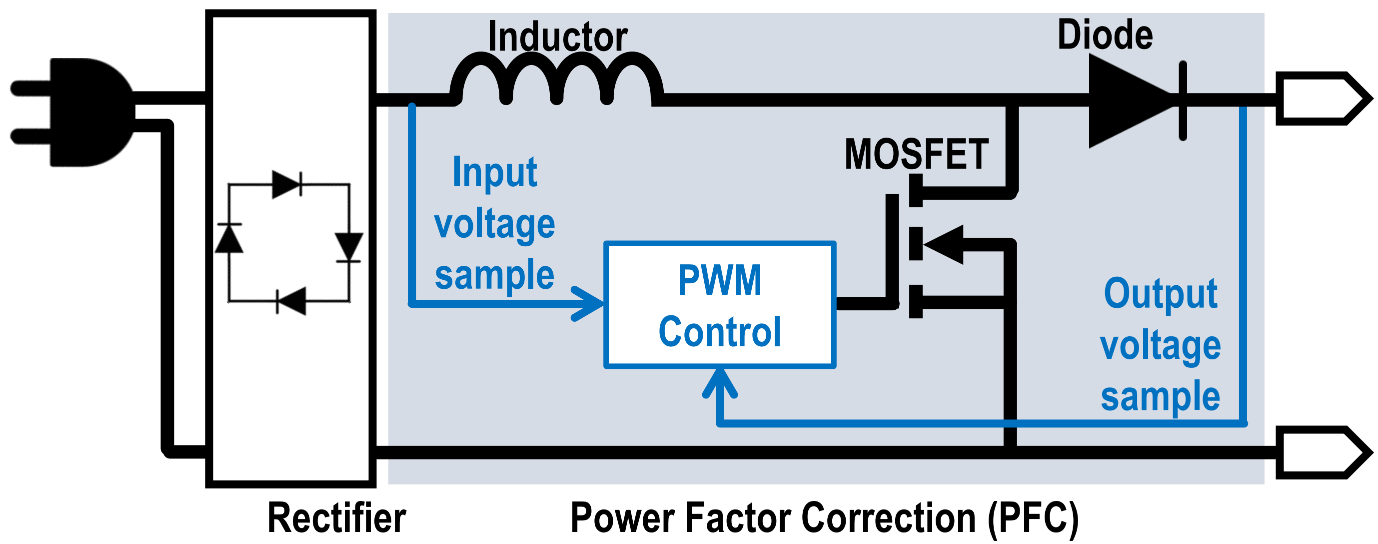


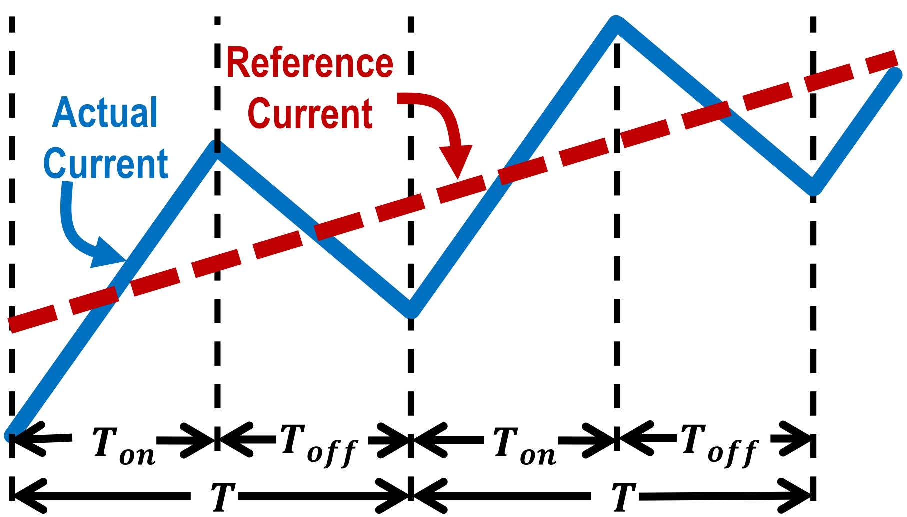
The ripples come from the PFC control



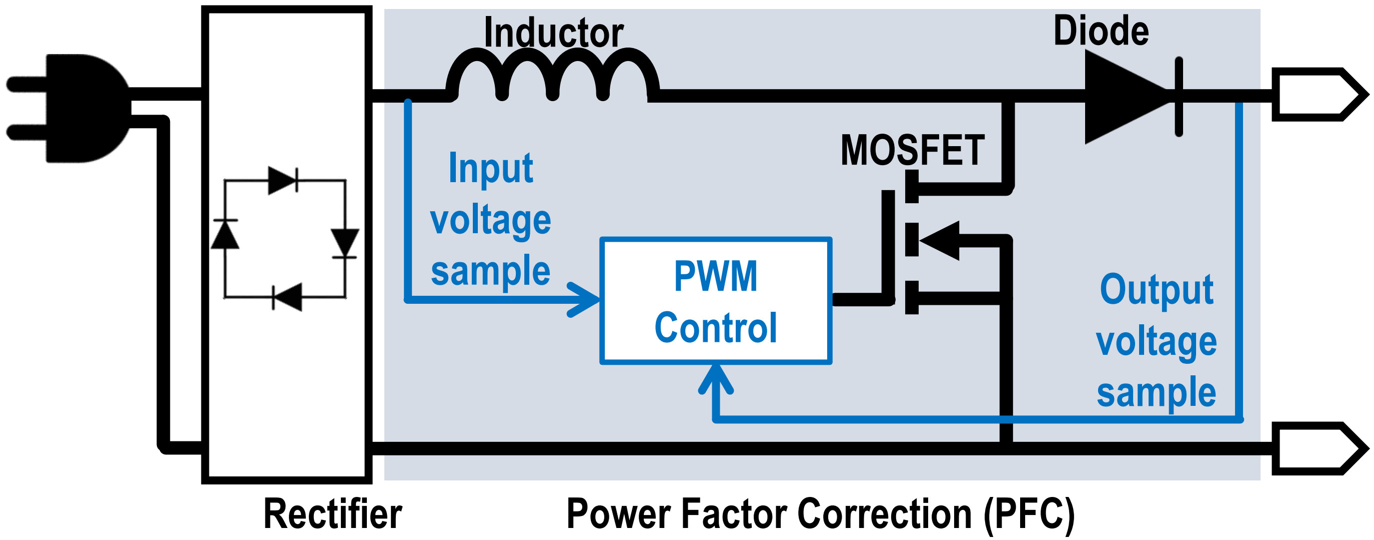


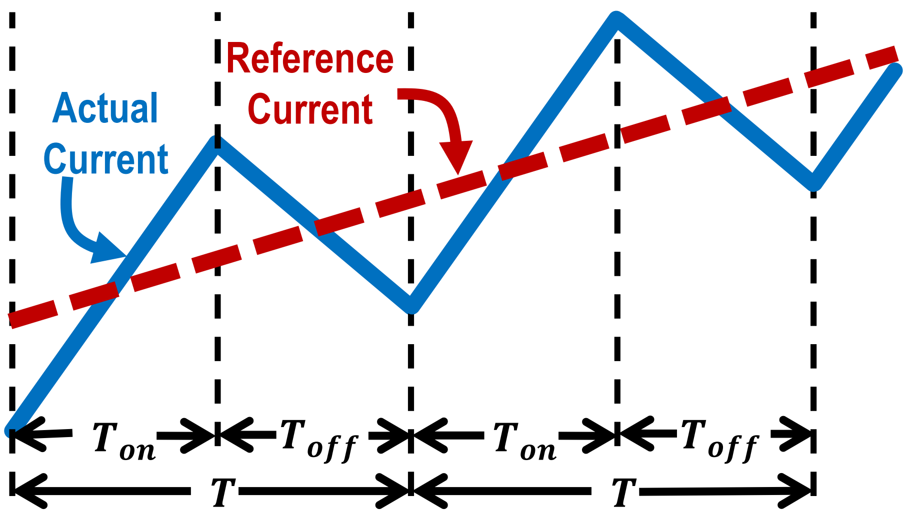
The ripples come from the PFC control

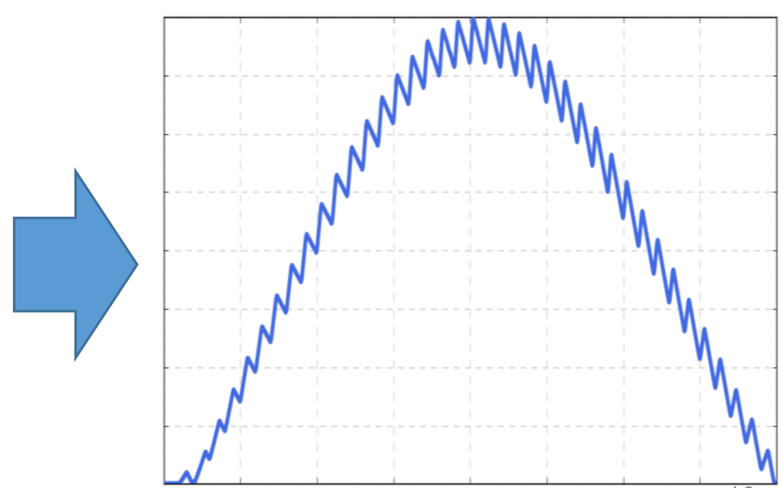




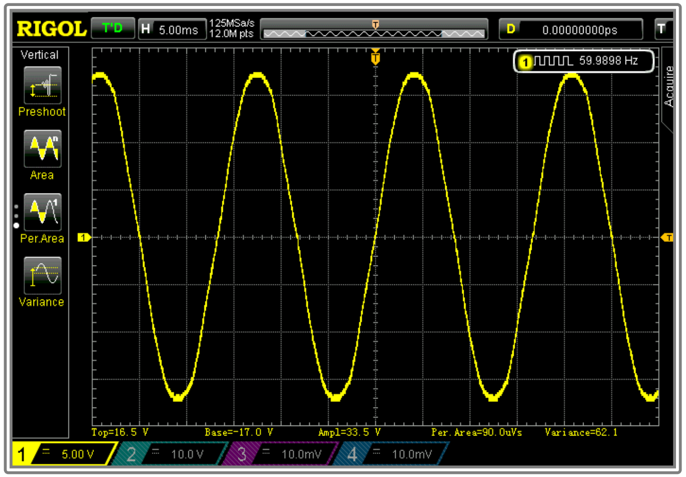
The ripples come from the PFC control



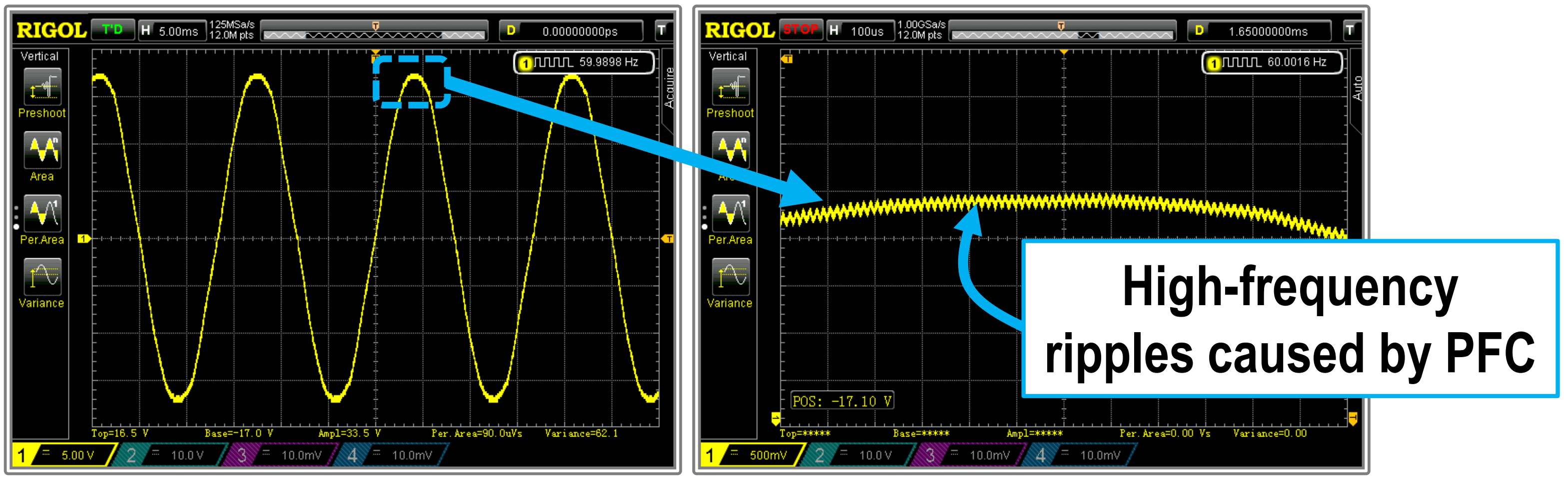




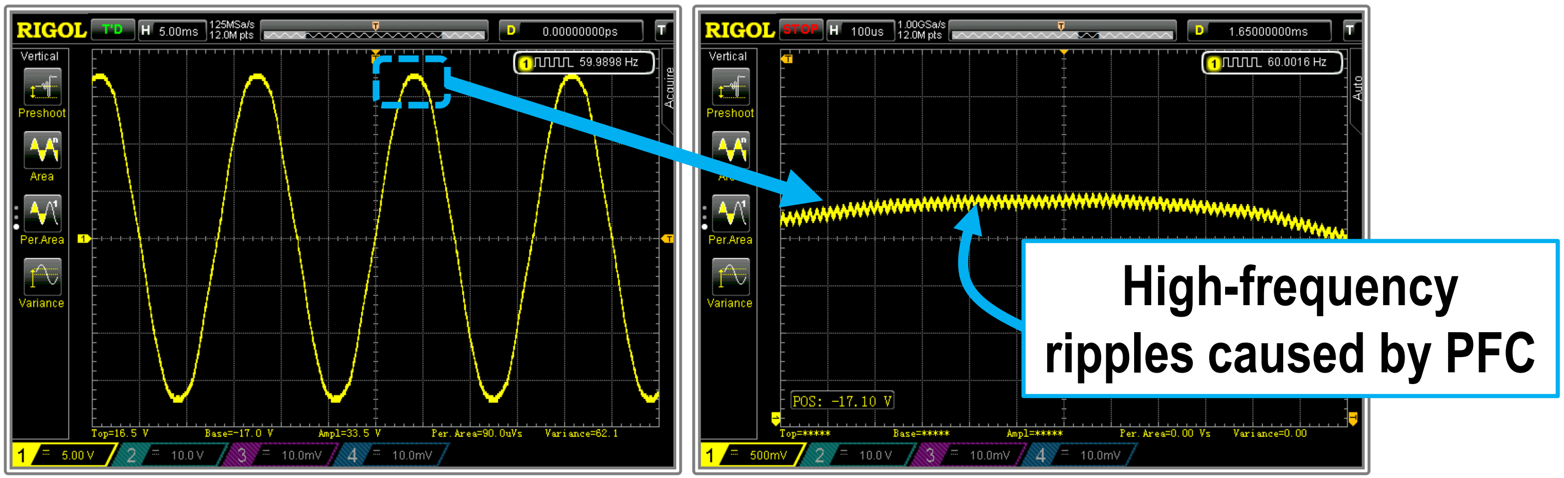
Voltage measurement of a Dell server



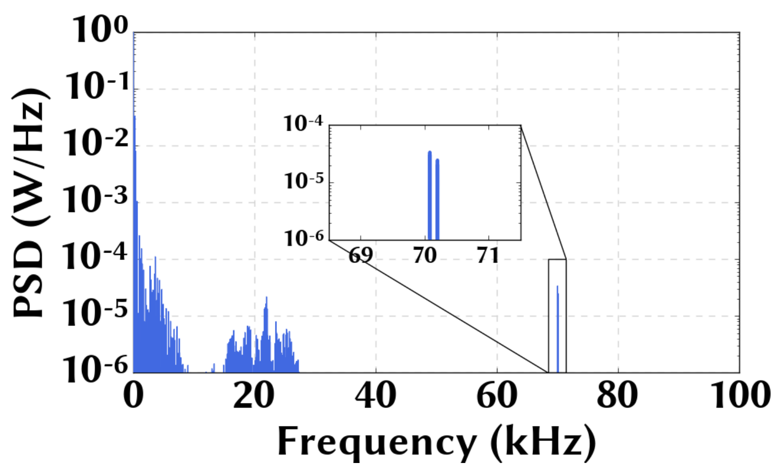
Voltage measurement of a Dell server



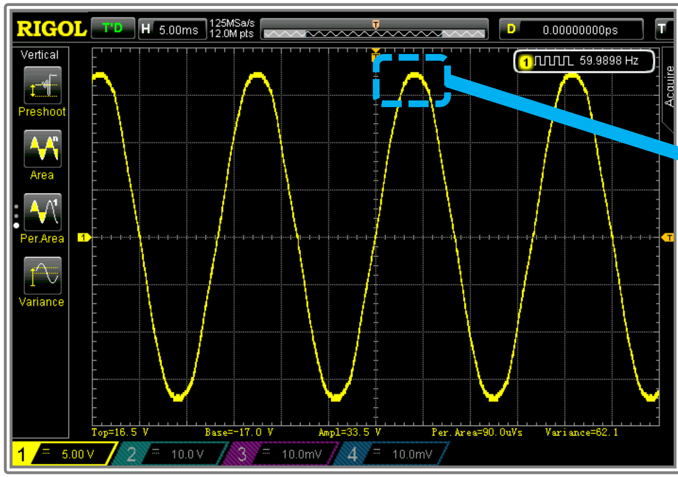
Voltage measurement of a Dell server

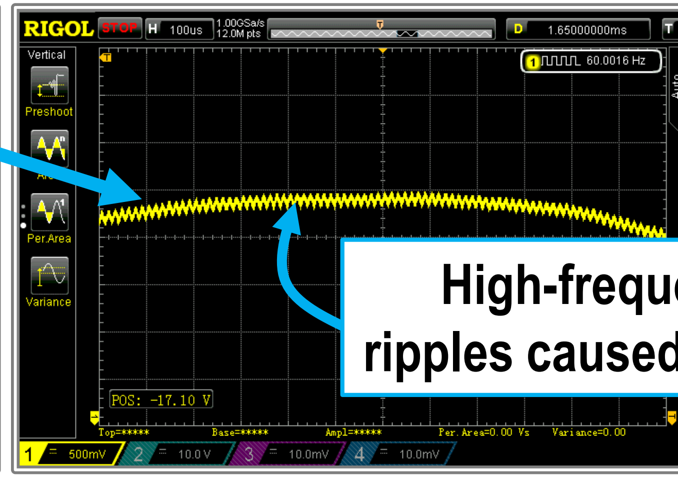


Frequency analysis of the voltage signal



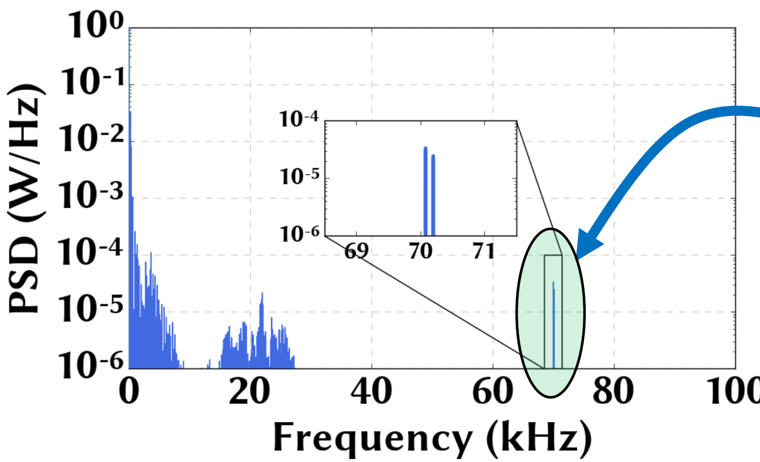
Voltage measurement of a Dell server





High-frequency ripples caused by PFC

Frequency analysis of the voltage signal



Frequency spike
(at PFC switching frequency)

Can we estimate the power load based on frequency spikes?

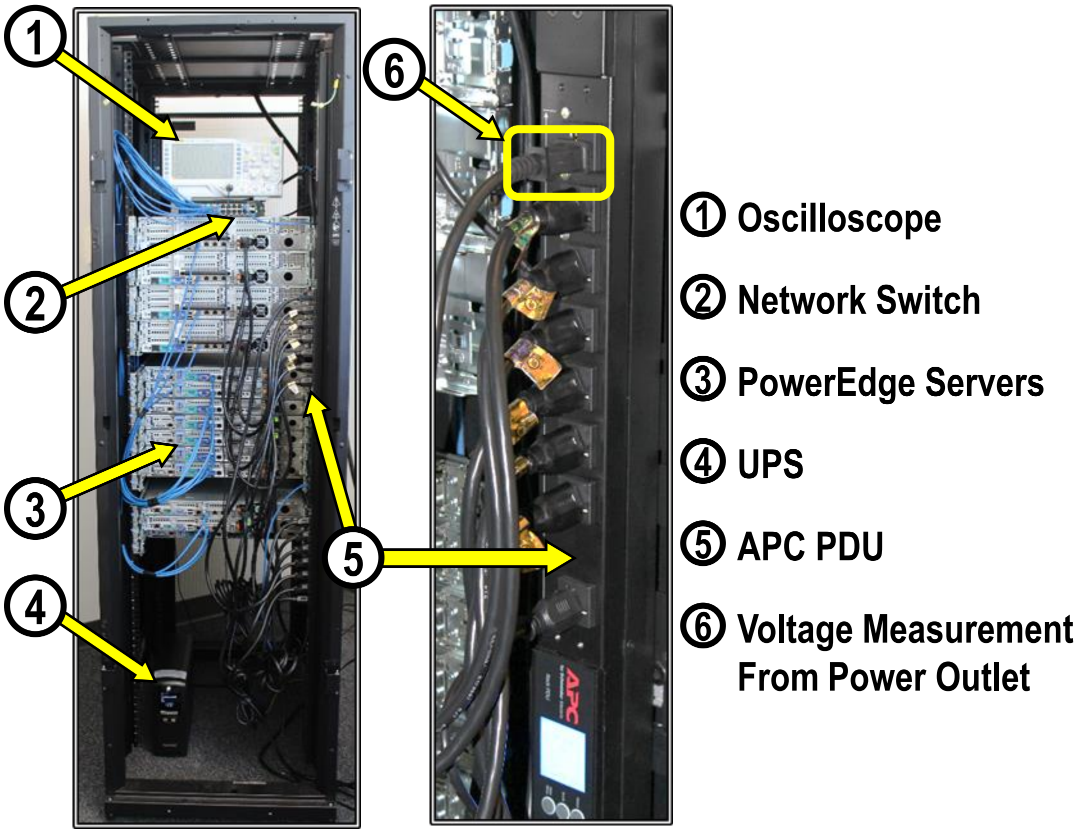
Can we estimate the power load based on frequency spikes?

Our intuition says "yes"!

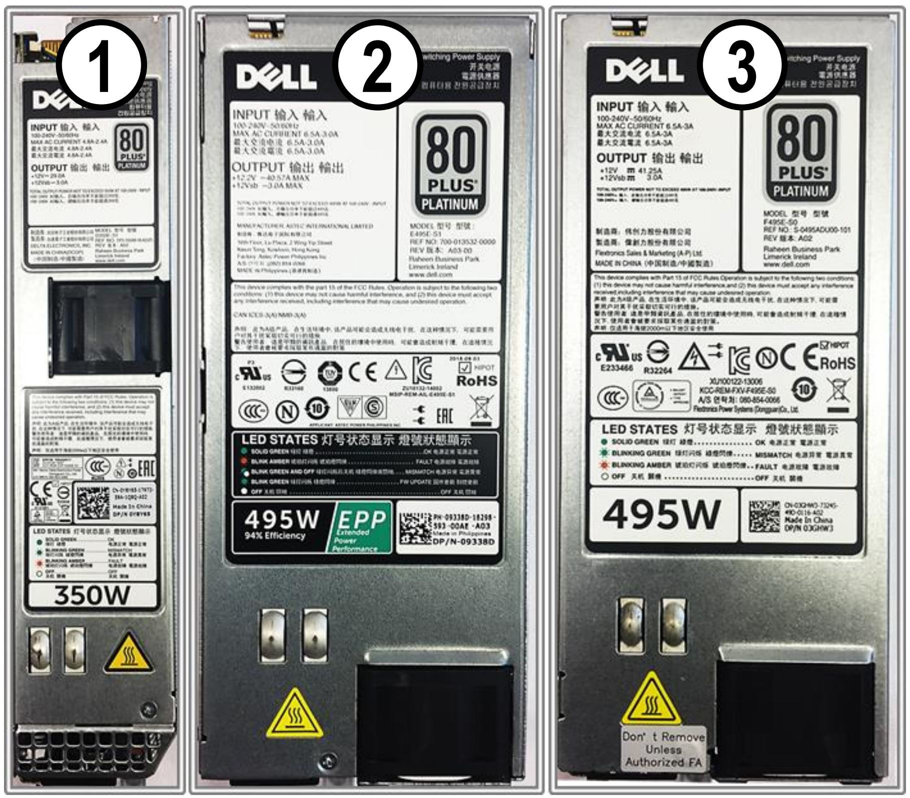
Given a higher current, the ripples need to rise up more during each cycle.

Experiment

- **13 Dell PowerEdge servers**
- **3 different server configurations**
- **3 different types of power supply units**



Power supplies

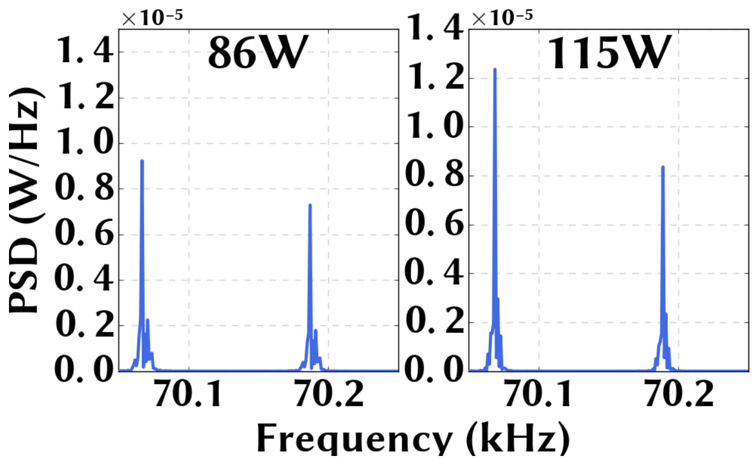


① 350W, PFC Switching ~63kHz
Model: D35E-S1
Manufacturer: Delta Electronics Inc.

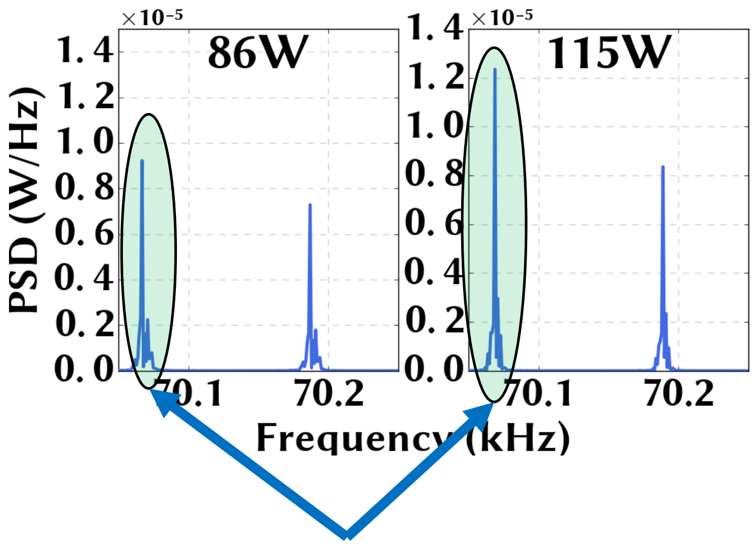
② 495W, PFC Switching ~66kHz
Model: F495E-S0
Manufacturer: Astec Intl. Ltd.

③ 495W, PFC Switching ~70kHz
Model: E495E-S1
Manufacturer: Flextronics Intl. Ltd.

PSD vs. server power

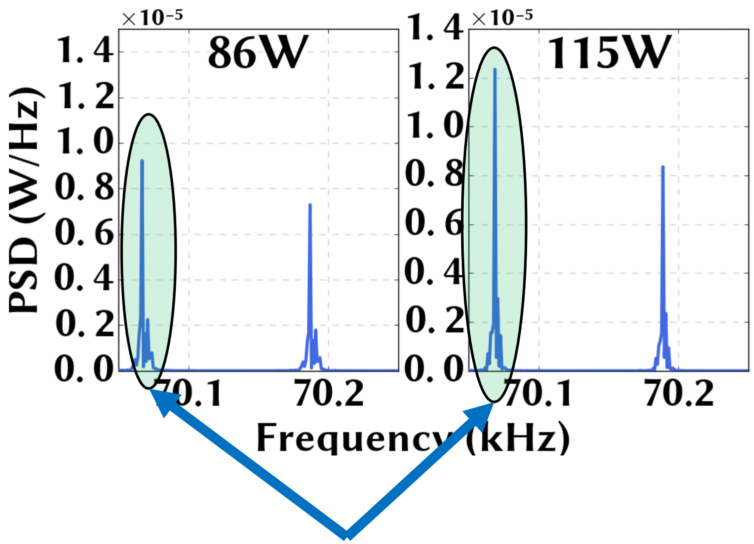


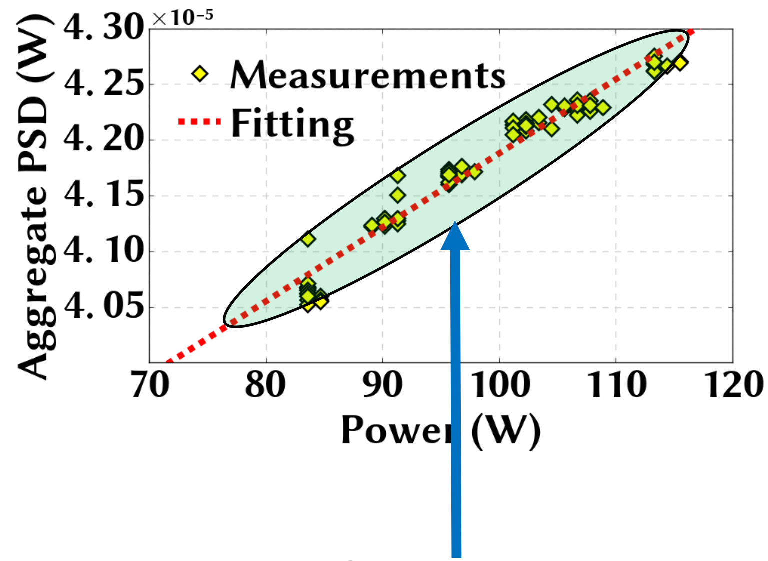
PSD vs. server power



Higher power creates taller frequency spikes

PSD vs. server power

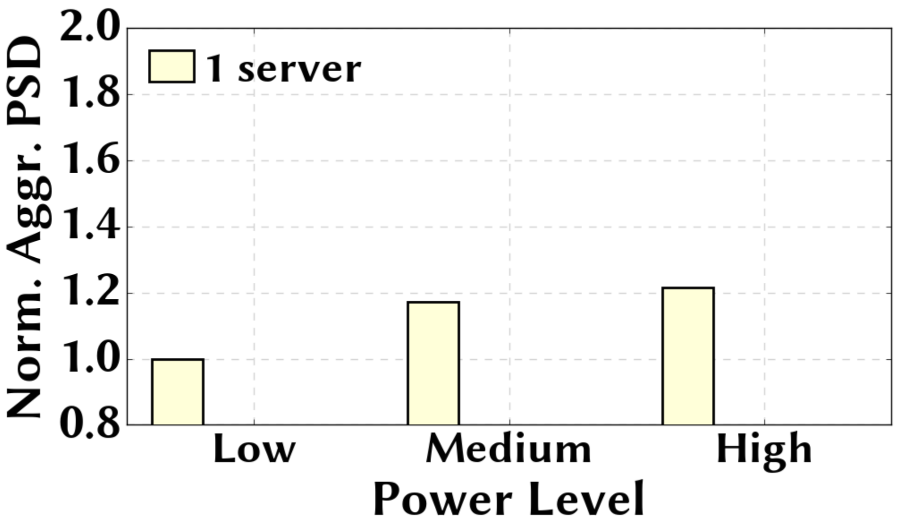




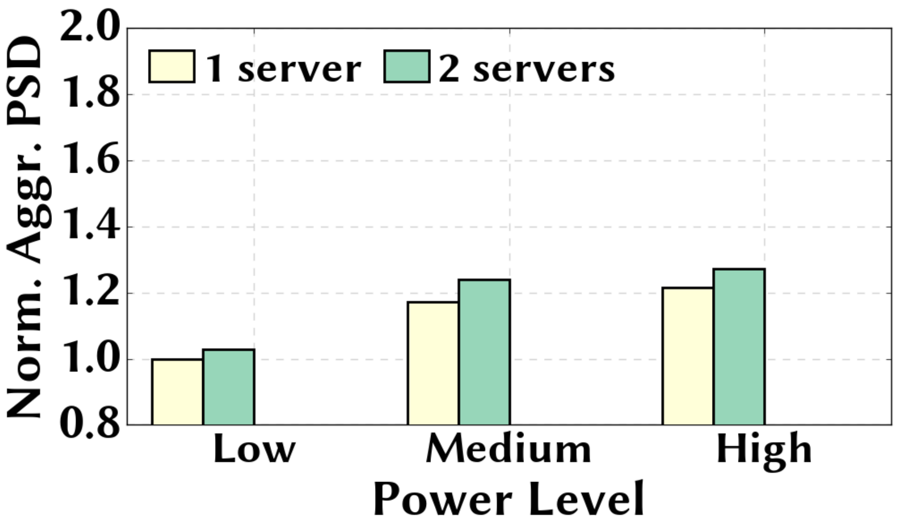
Higher power creates taller frequency spikes

Aggregate PSD monotonically increases with server power

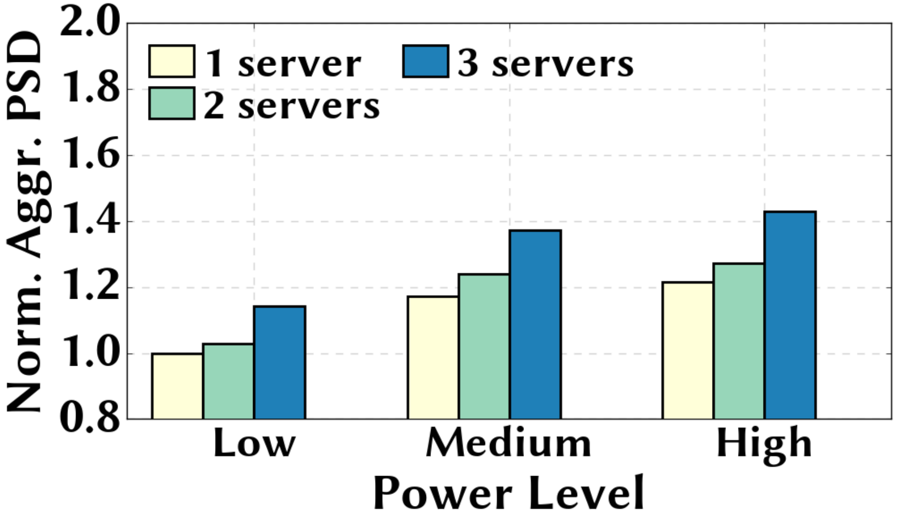
PSD vs. server power



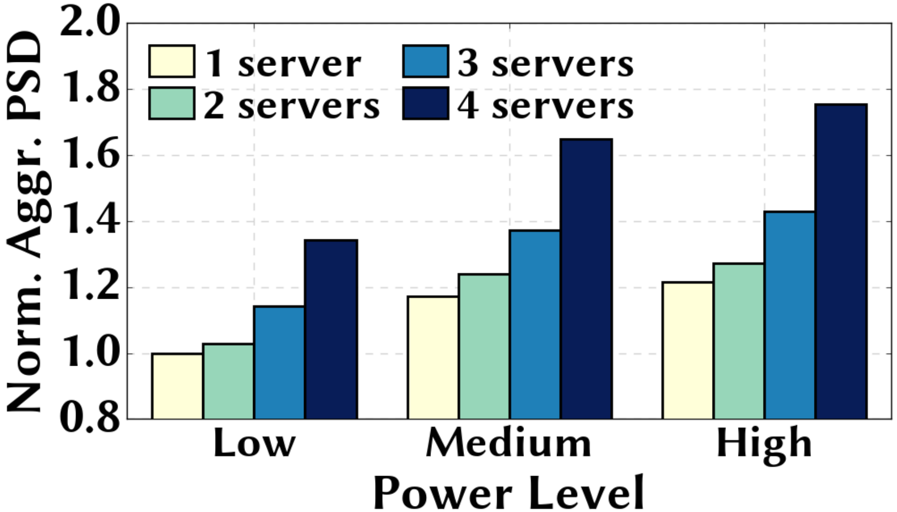
PSD vs. server power



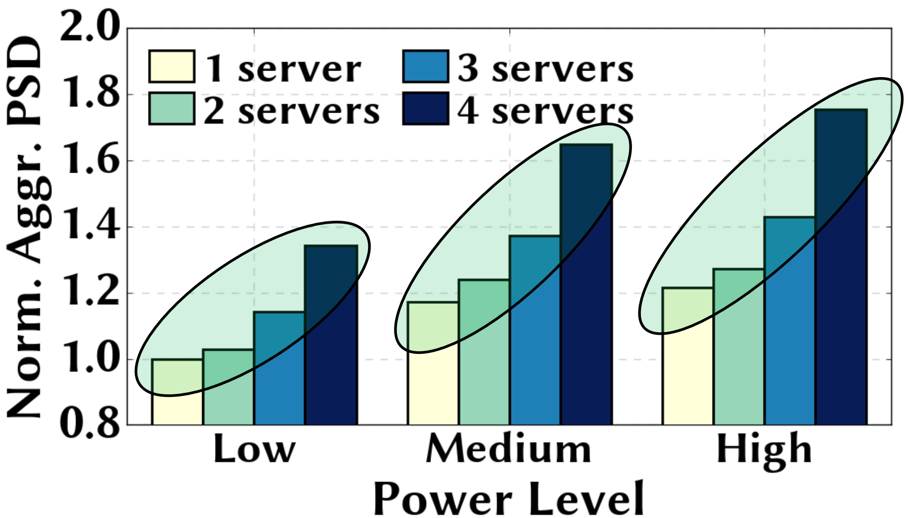
PSD vs. server power



PSD vs. server power

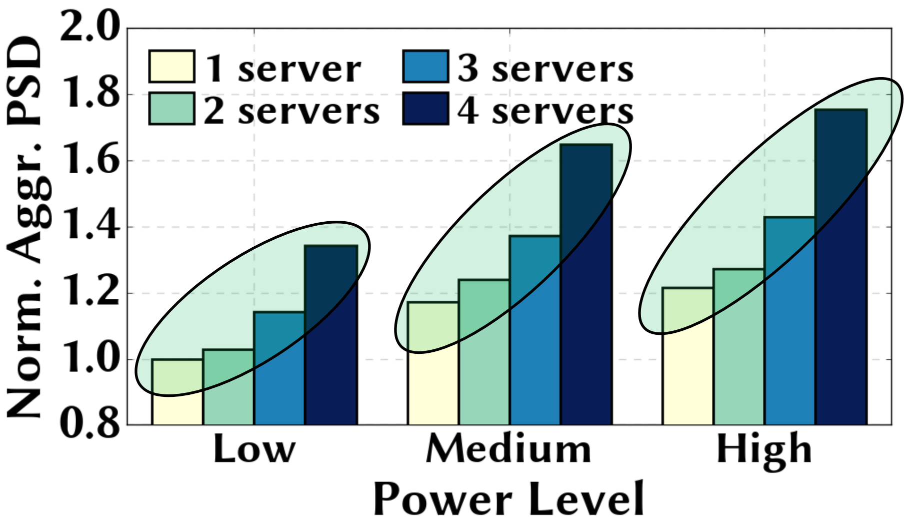


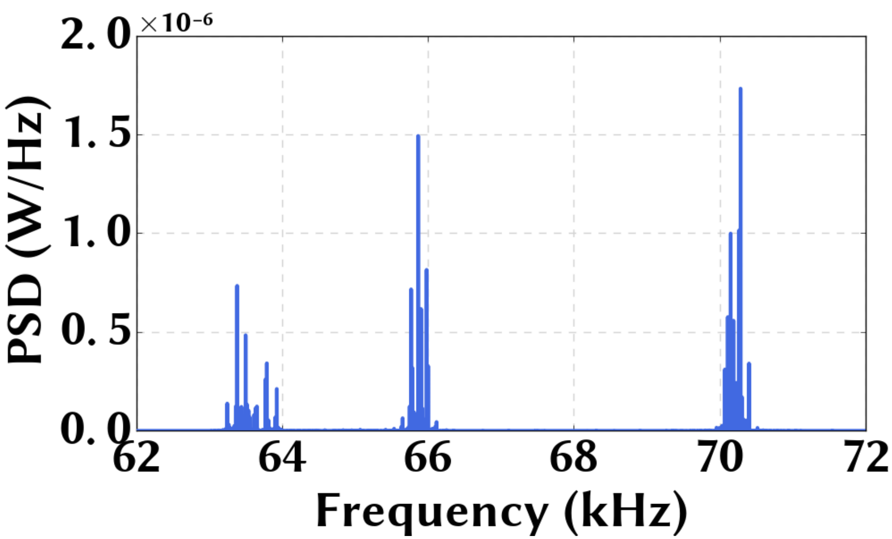
PSD vs. server power



Aggregate PSD is additive for multiple servers with similar PFC frequencies

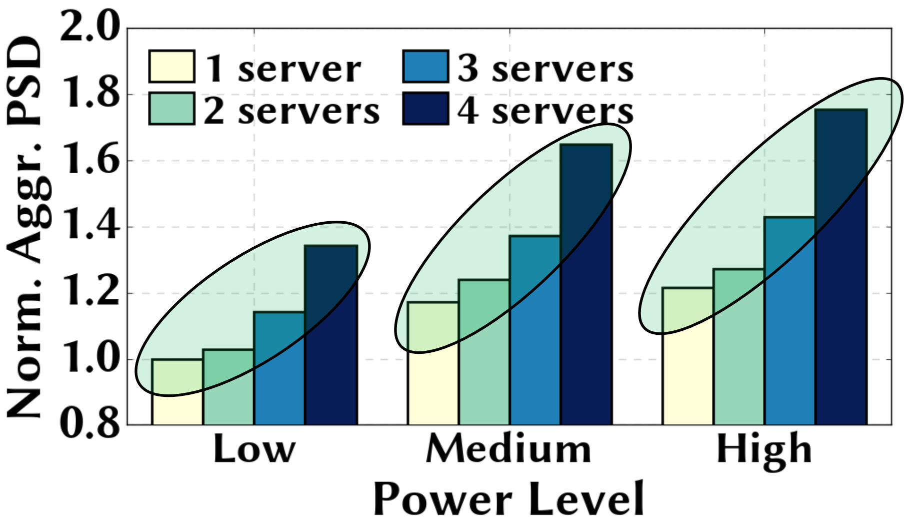
PSD vs. server power



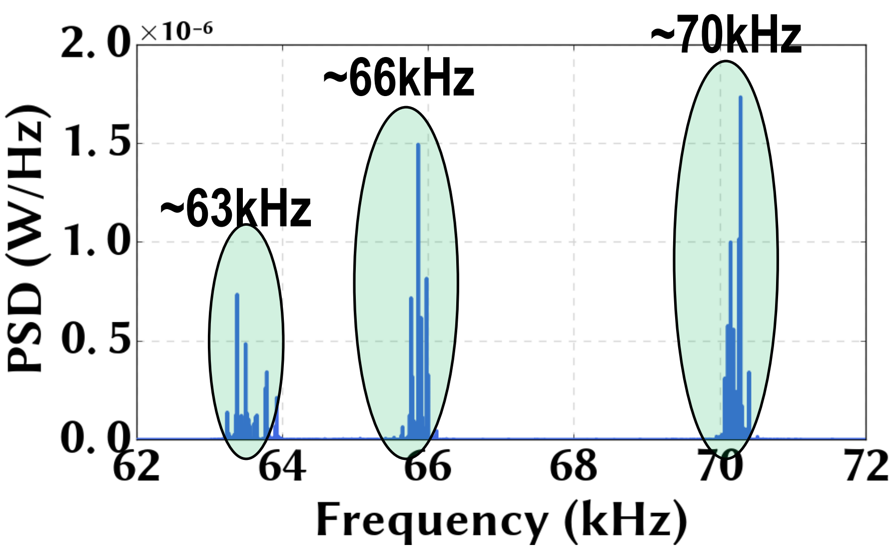


Aggregate PSD is additive for multiple servers with similar PFC frequencies

PSD vs. server power

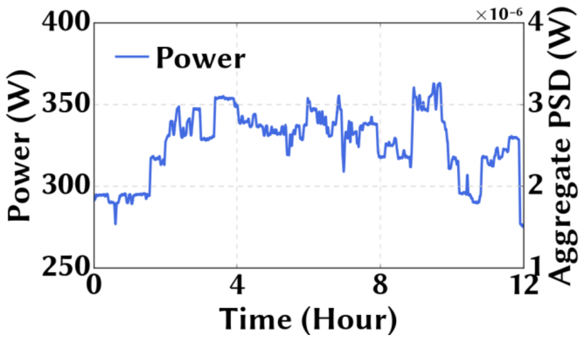


Aggregate PSD is additive for multiple servers with similar PFC frequencies

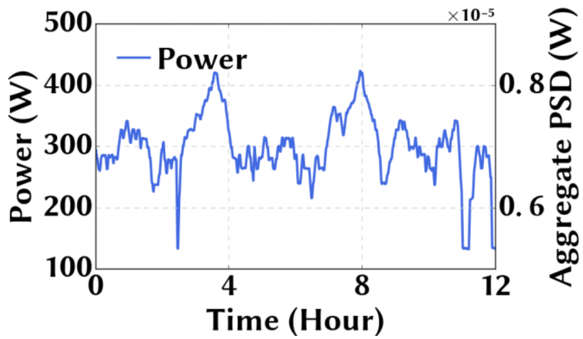


Frequency spikes are separated for different types of power supply units

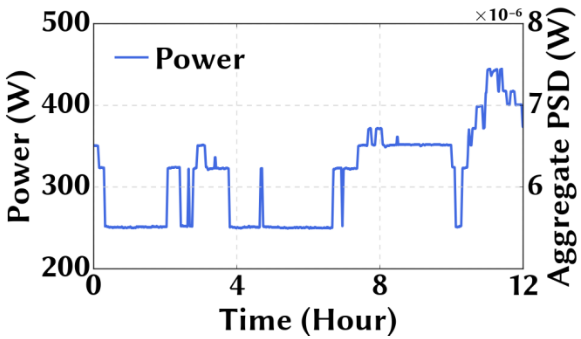
Accuracy of the voltage side channel



Tenant #1

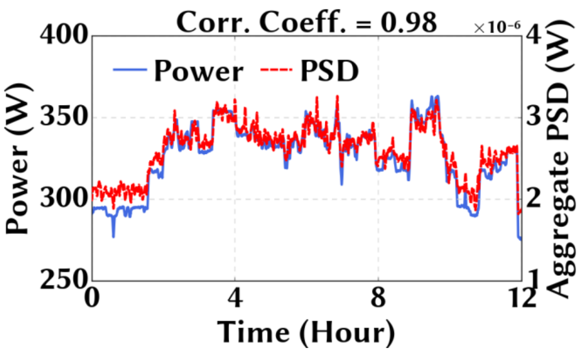


Tenant #2

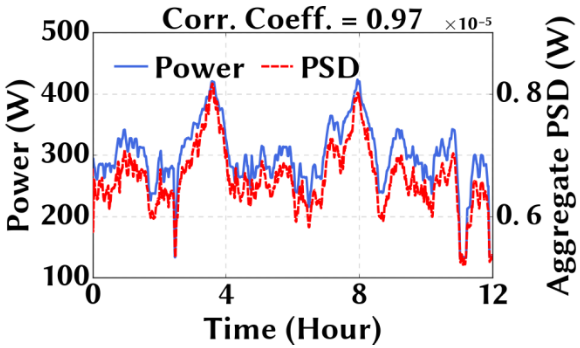


Tenant #3

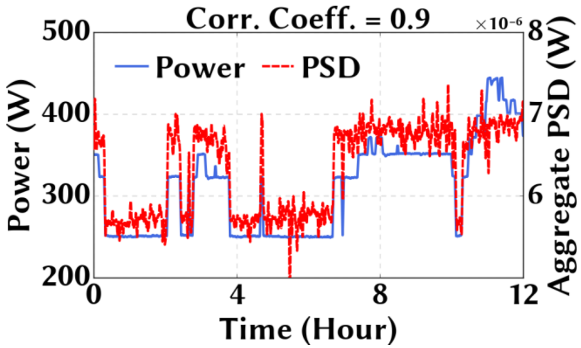
Accuracy of the voltage side channel



Tenant #1



Tenant #2

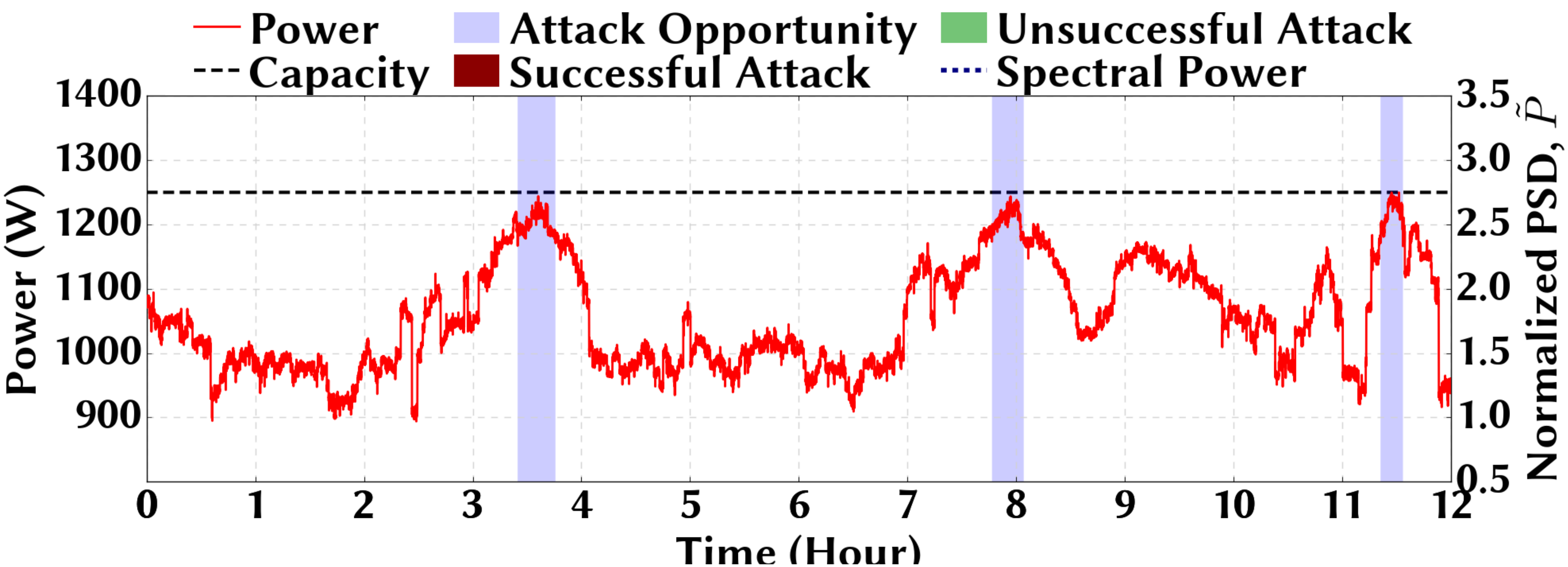


Tenant #3

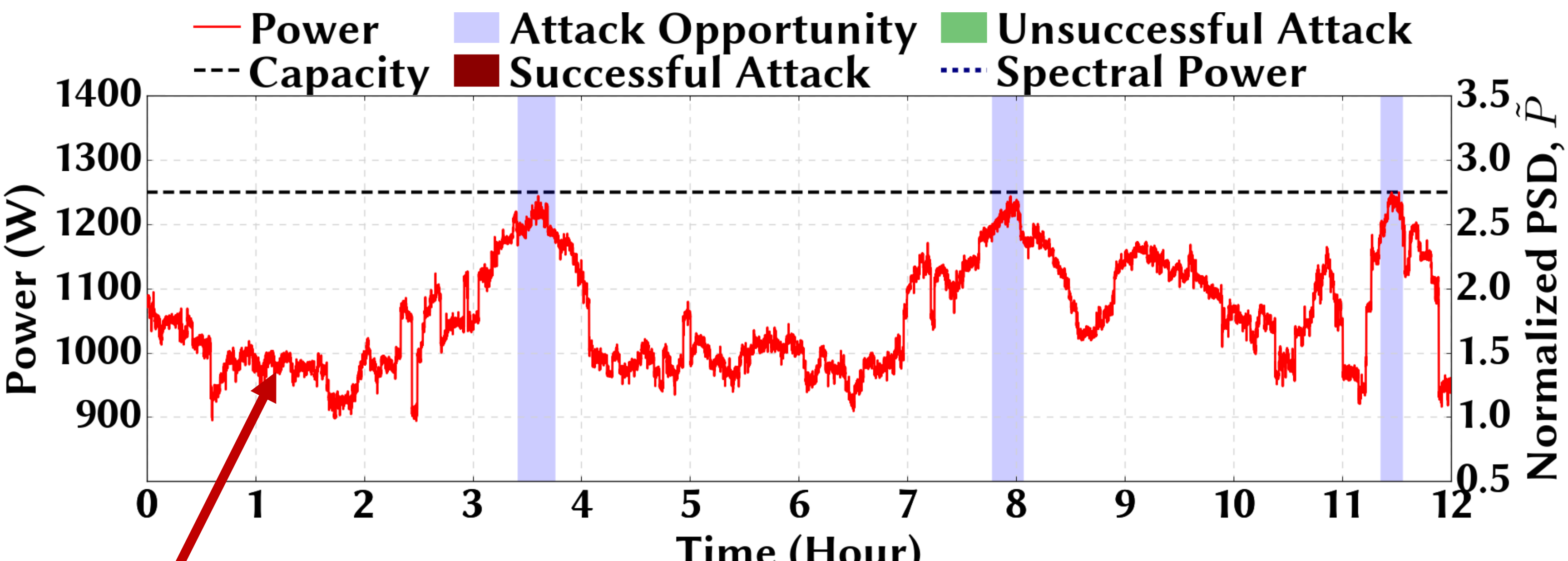
Estimating power loads with a high accuracy!

Attack only when the estimated power load is sufficiently high

Power attack

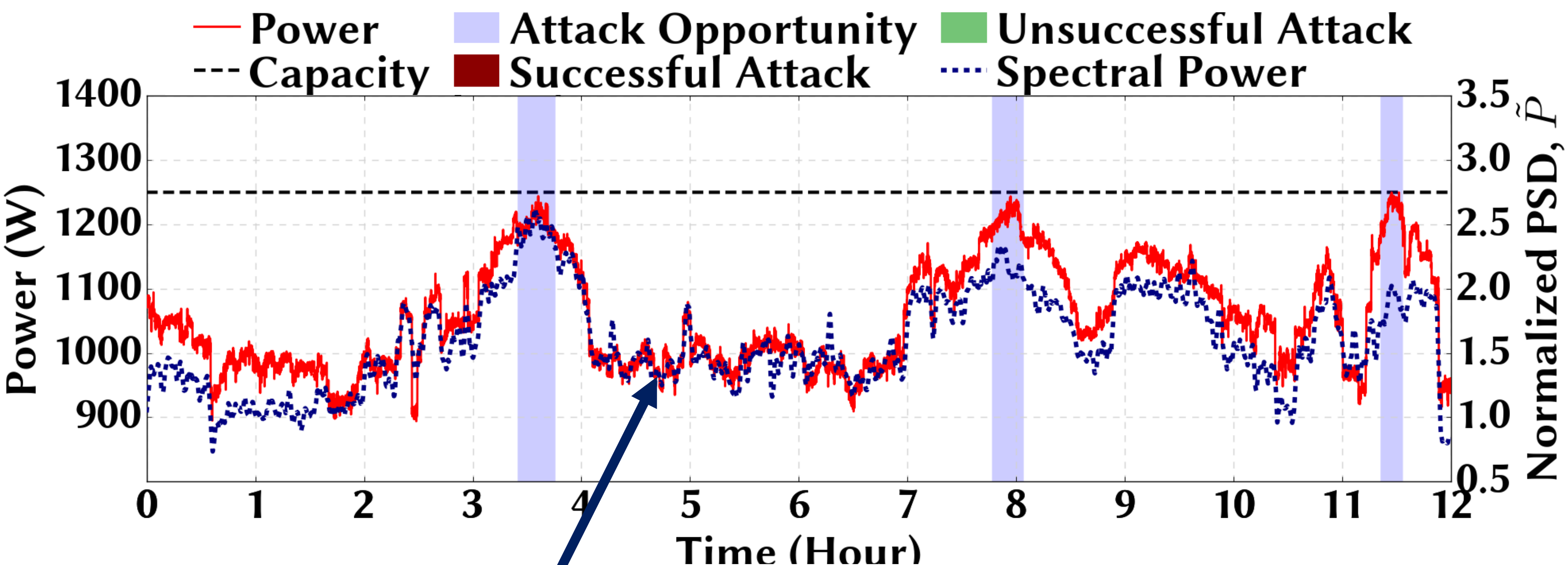


Power attack



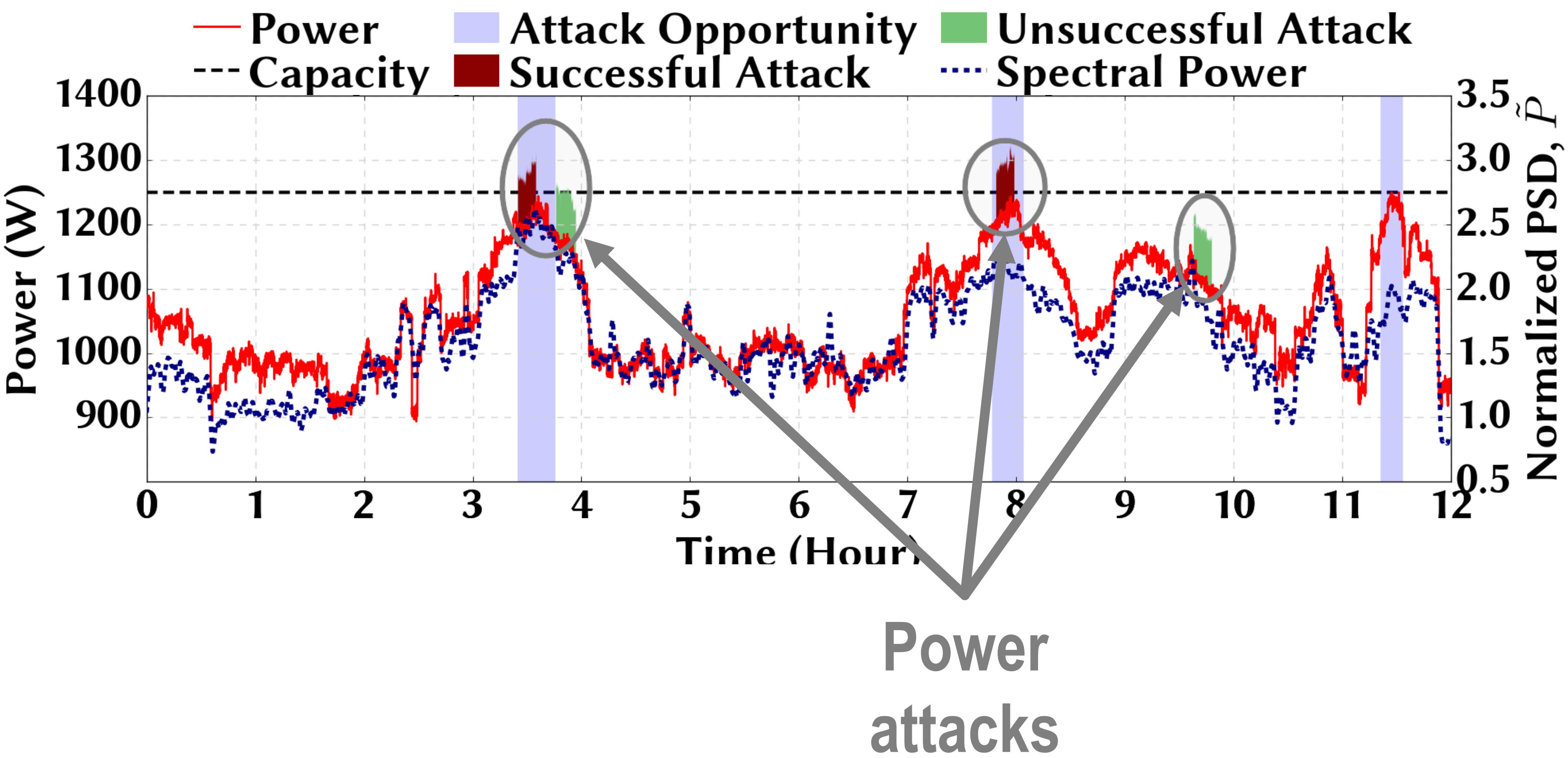
Tenants' total power

Power attack

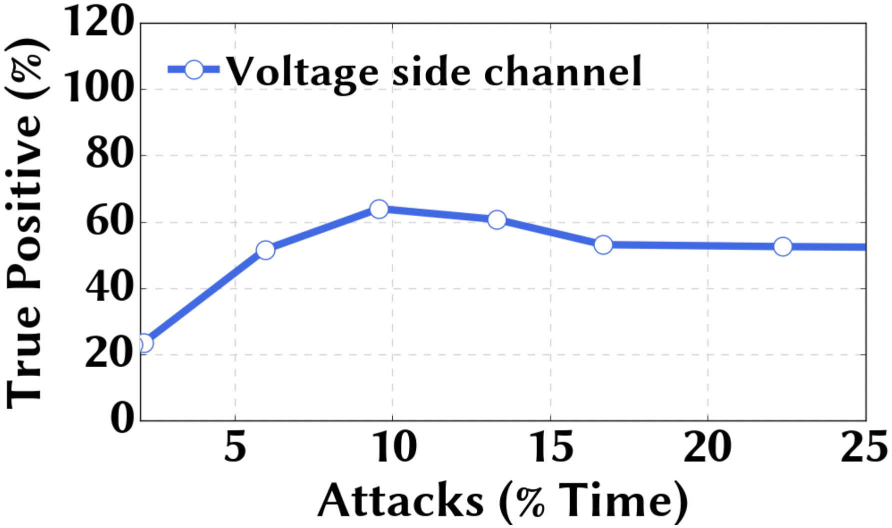


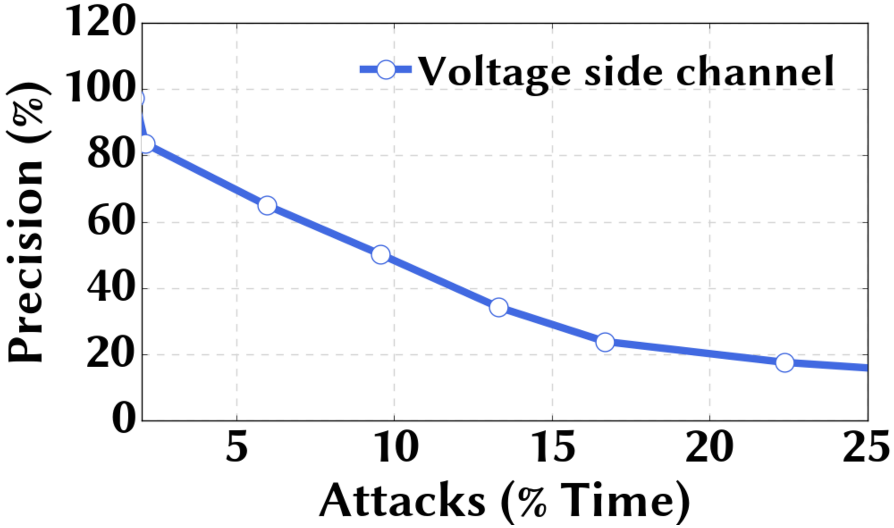
Estimated power loads

Power attack

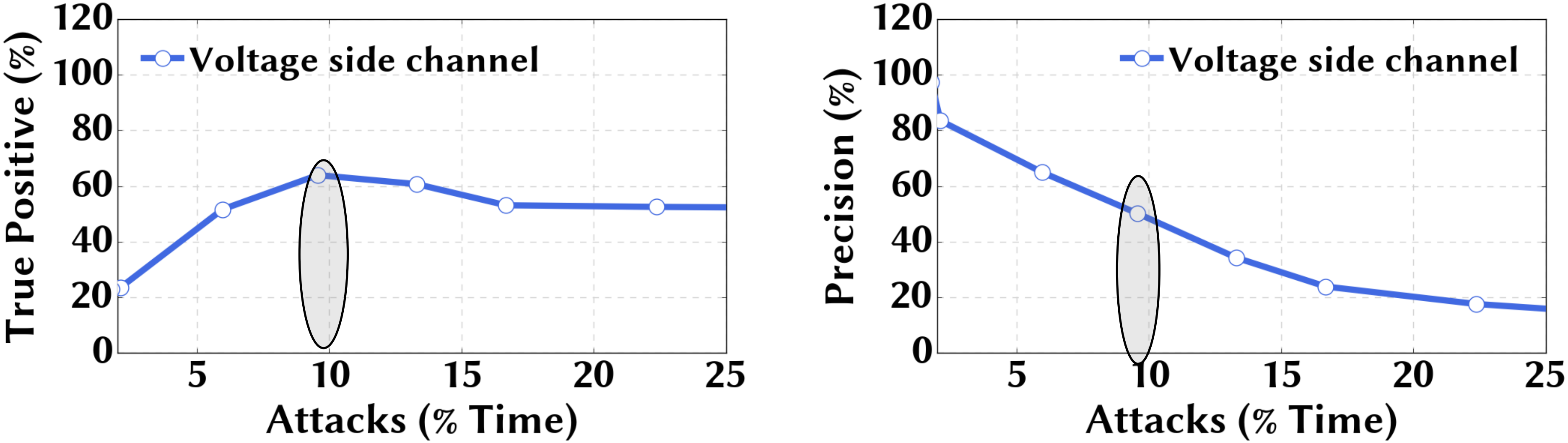


Timing accuracy



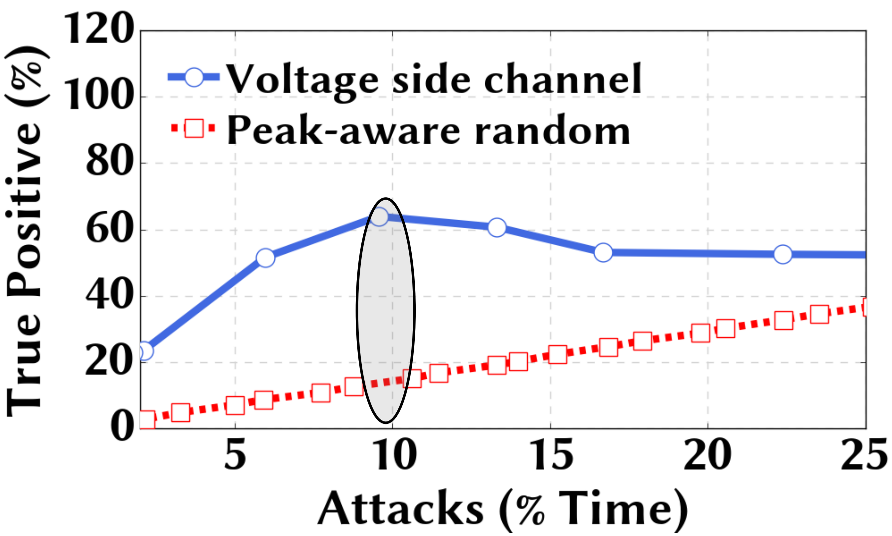


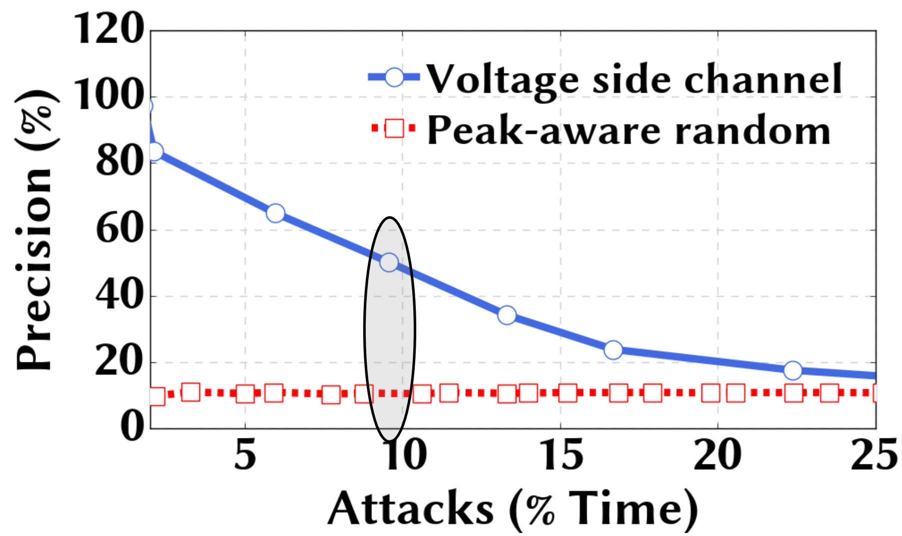
Timing accuracy



>50% true positive rate and precision for ~10% attack

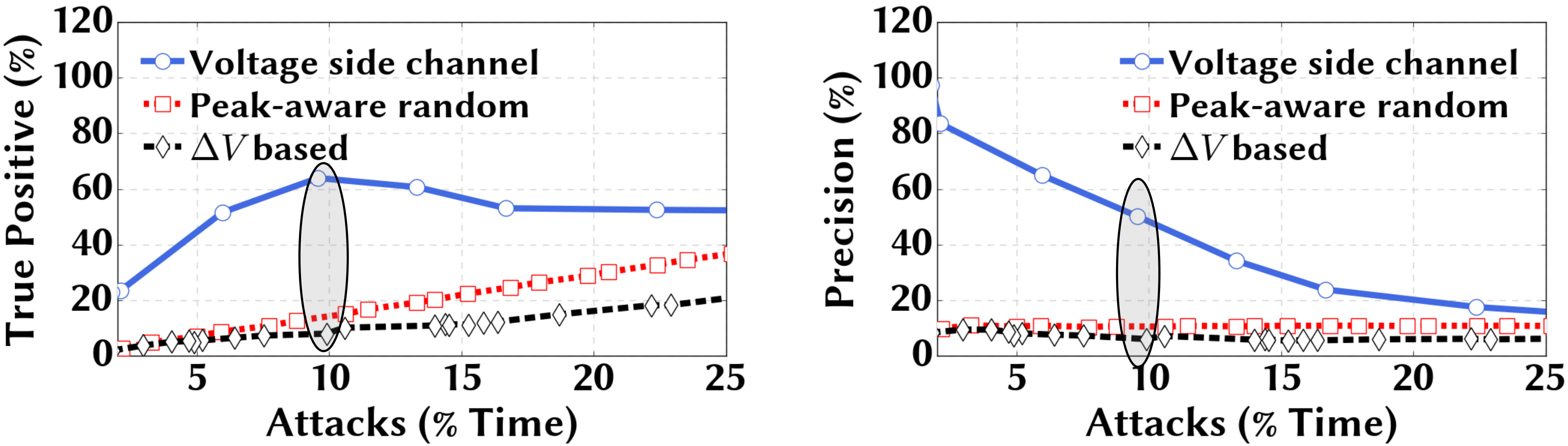
Timing accuracy





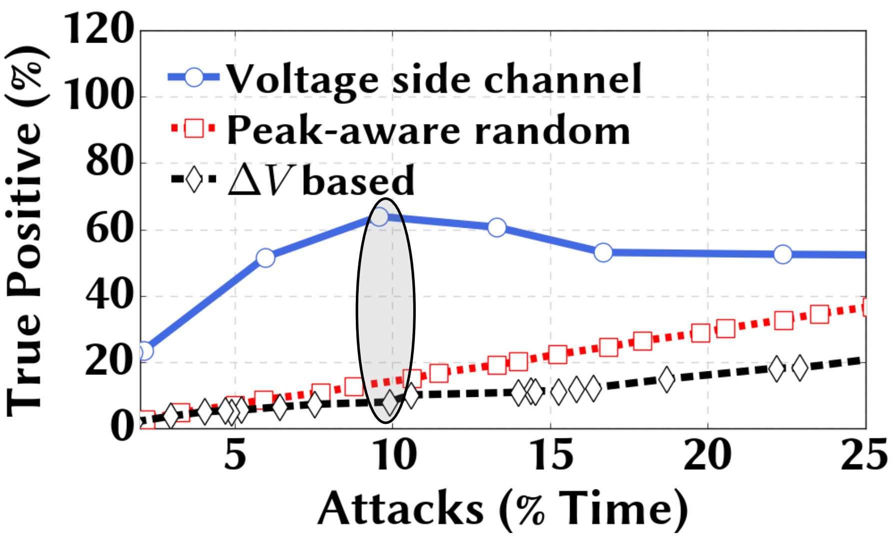
>50% true positive rate and precision for ~10% attack

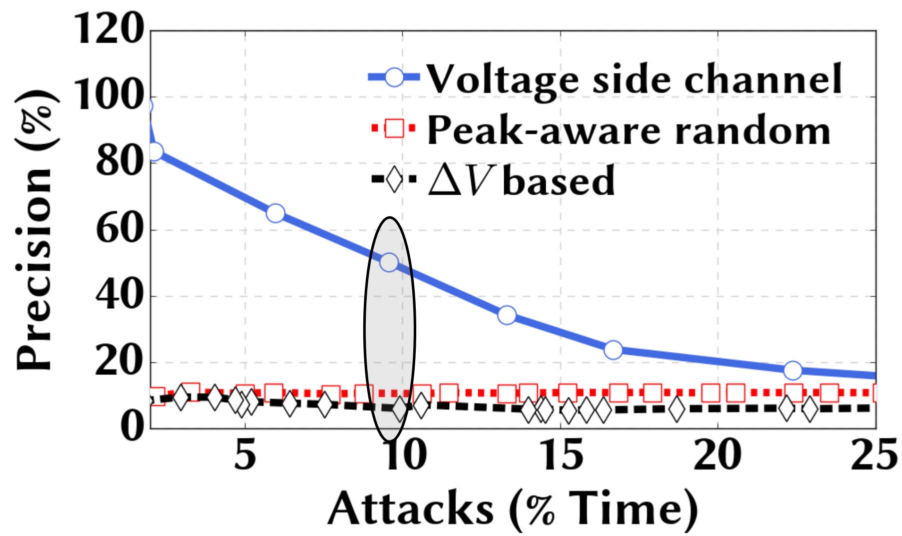
Timing accuracy



>50% true positive rate and precision for ~10% attack

Timing accuracy

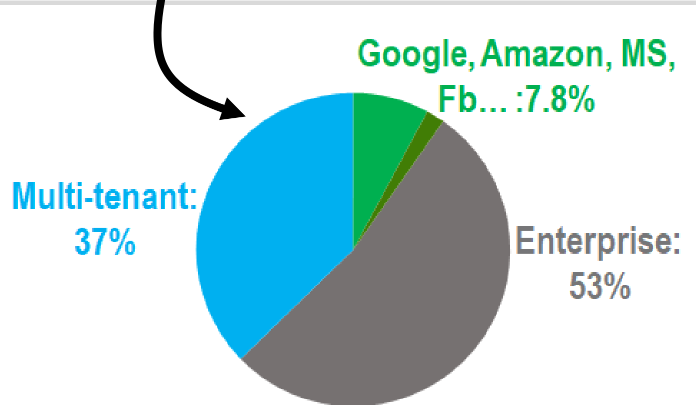




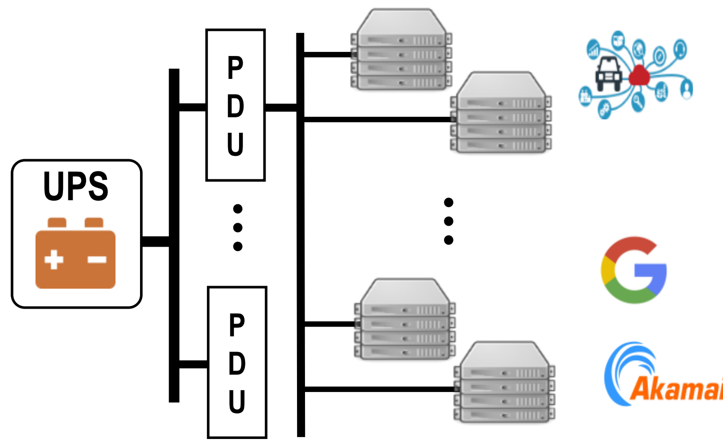
>50% true positive rate and precision for ~10% attack

Also works with UPS and three-phase power systems

Physical infrastructure sharing means everything but power security



Percentage of electricity usage by data center type (source: NRDC 2015)



Thanks!

References

- M. A. Islam, **S. Ren**, and A. Wierman, "Exploiting a Thermal Side Channel for Power Attacks in Multi-Tenant Data Centers," ACM Conference on Computer and Communications Security (**CCS**), 2017.
- M. A. Islam, L. Yang, K. Ranganath, and **S. Ren**, "Why Some Like It Loud: Timing Power Attacks in Multi-tenant Data Centers Using an Acoustic Side Channel," ACM International Conference on Measurement and Modeling of Computer Systems (**SIGMETRICS**), 2018.
- M. A. Islam and **S. Ren**, "Ohm's Law in Data Centers: A Voltage Side Channel for Timing Power Attacks," ACM Conference on Computer and Communications Security (**CCS**), 2018.