Why Some Like It Loud:

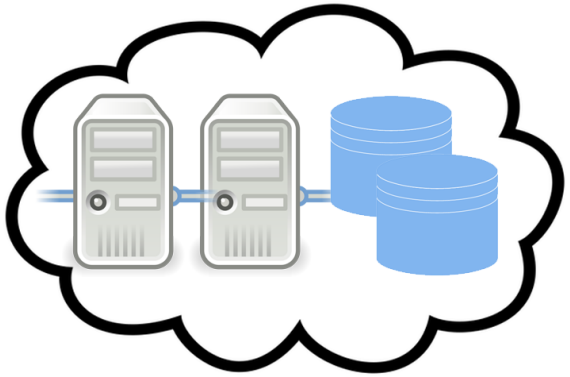
Timing Power Attacks in Multi-tenant Data Centers Using an Acoustic Side Channel

Mohammad A. Islam, Luting Yang, Kiran Ranganath, and Shaolei Ren

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

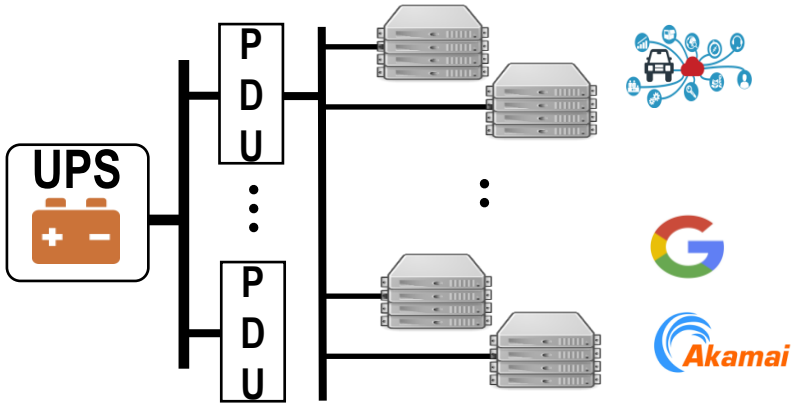
This talk is NOT about multi-tenant clouds;
it's about multi-tenant data centers!

This talk is NOT about multi-tenant clouds; it's about multi-tenant data centers!



Tenant = virtual machines

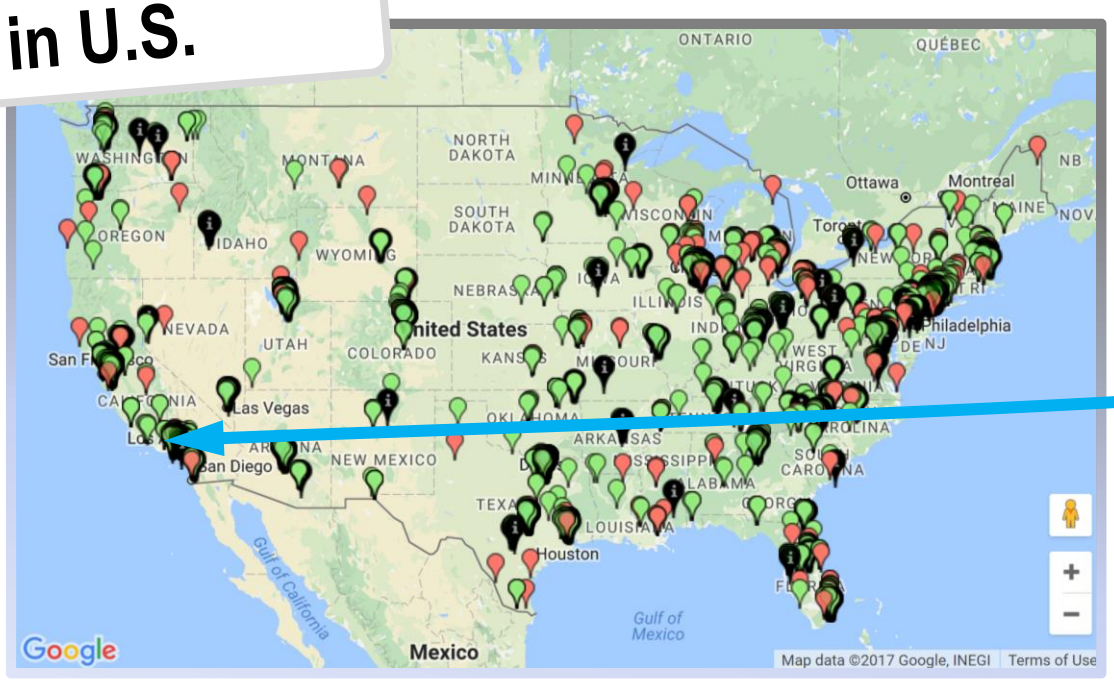
vs

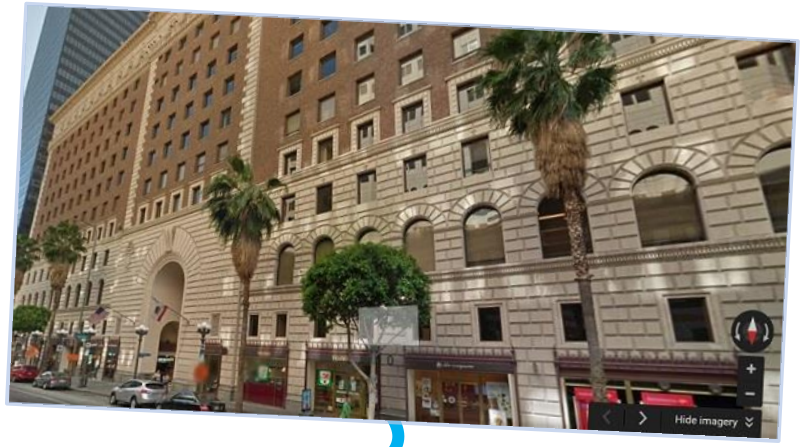


Tenant = **physical** servers

Multi-tenant data centers are everywhere…

2,000+ in U.S.

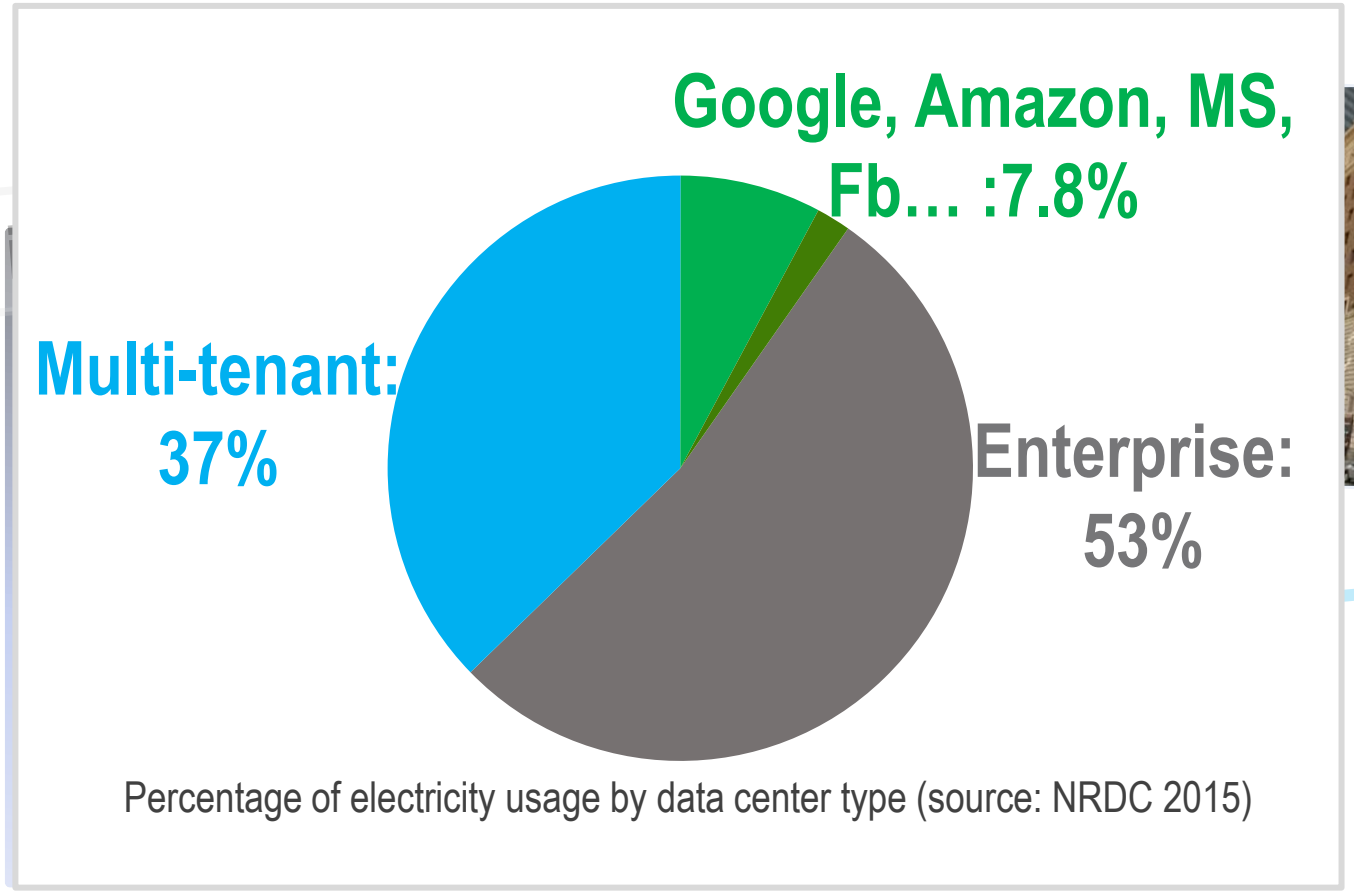




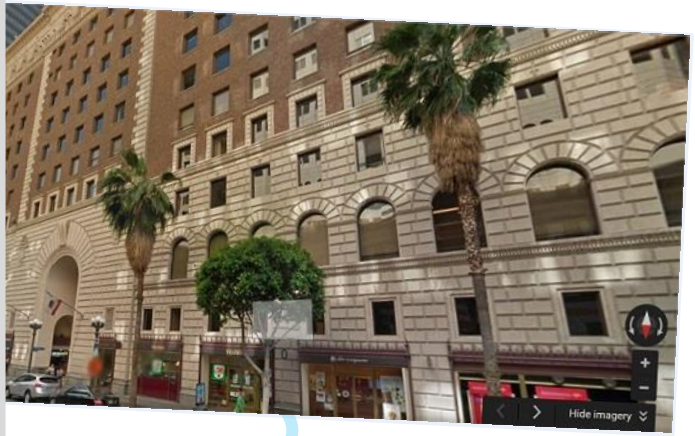
Apple houses 25% of its servers in multi-tenant data centers…

Multi-tenant data centers are everywhere…

2,000+

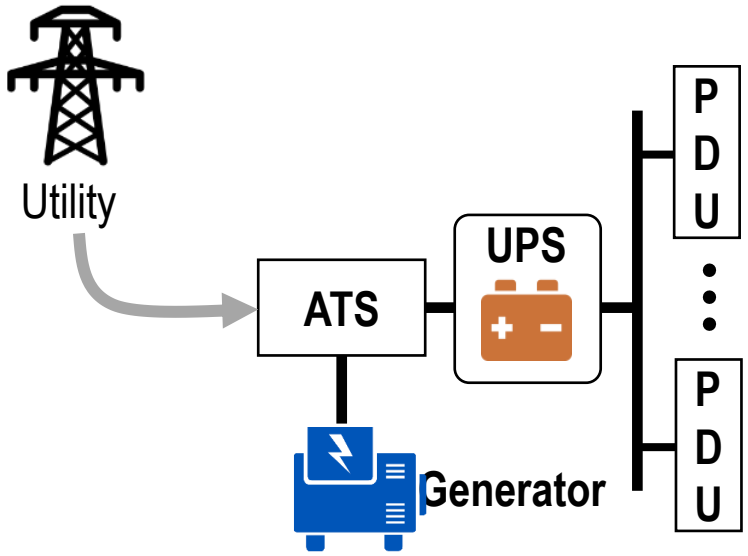


Percentage of electricity usage by data center type (source: NRDC 2015)

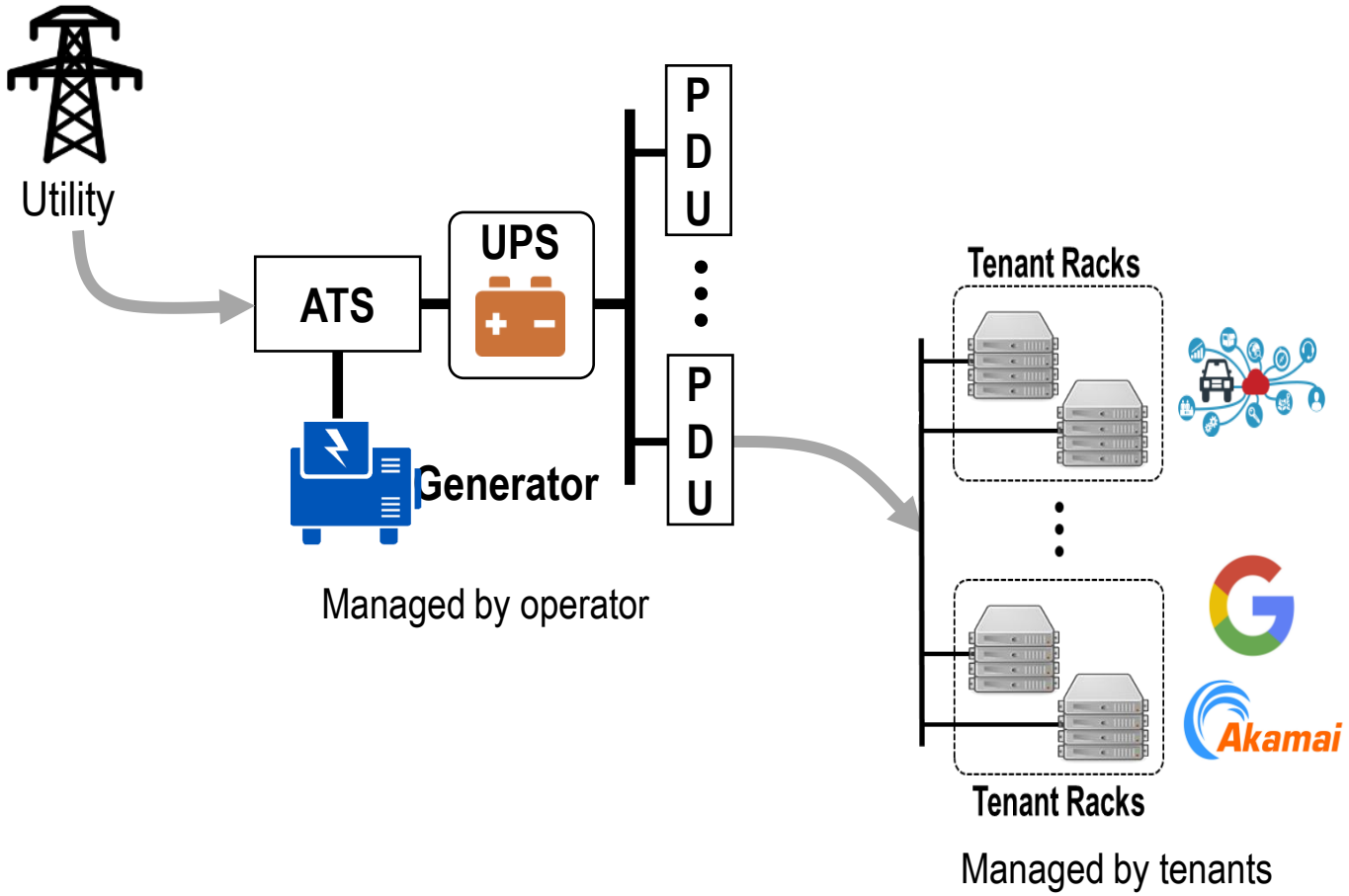


Apple houses 25% of its servers in multi-tenant data centers…

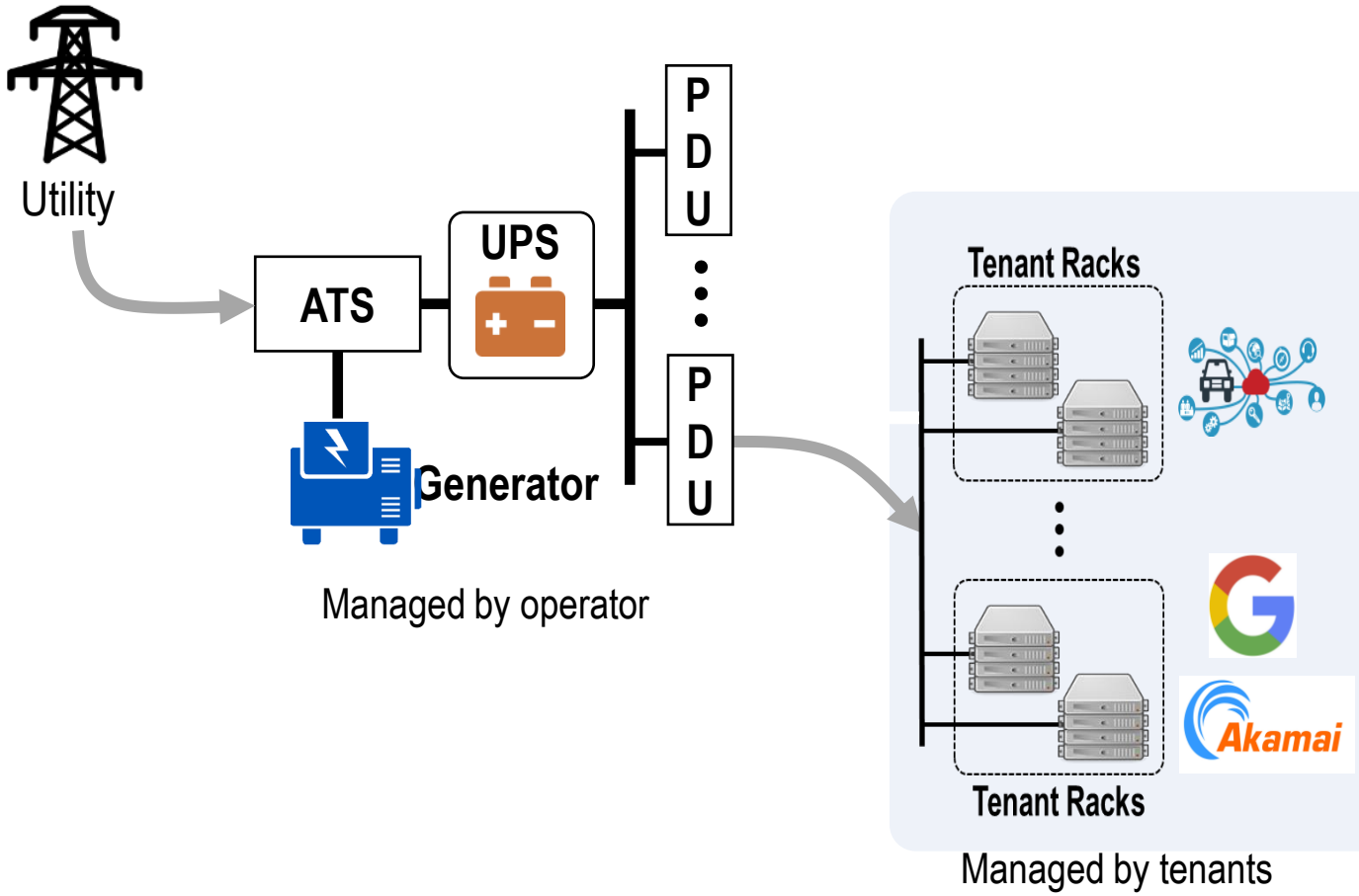
An overview of multi-tenant data center



An overview of multi-tenant data center



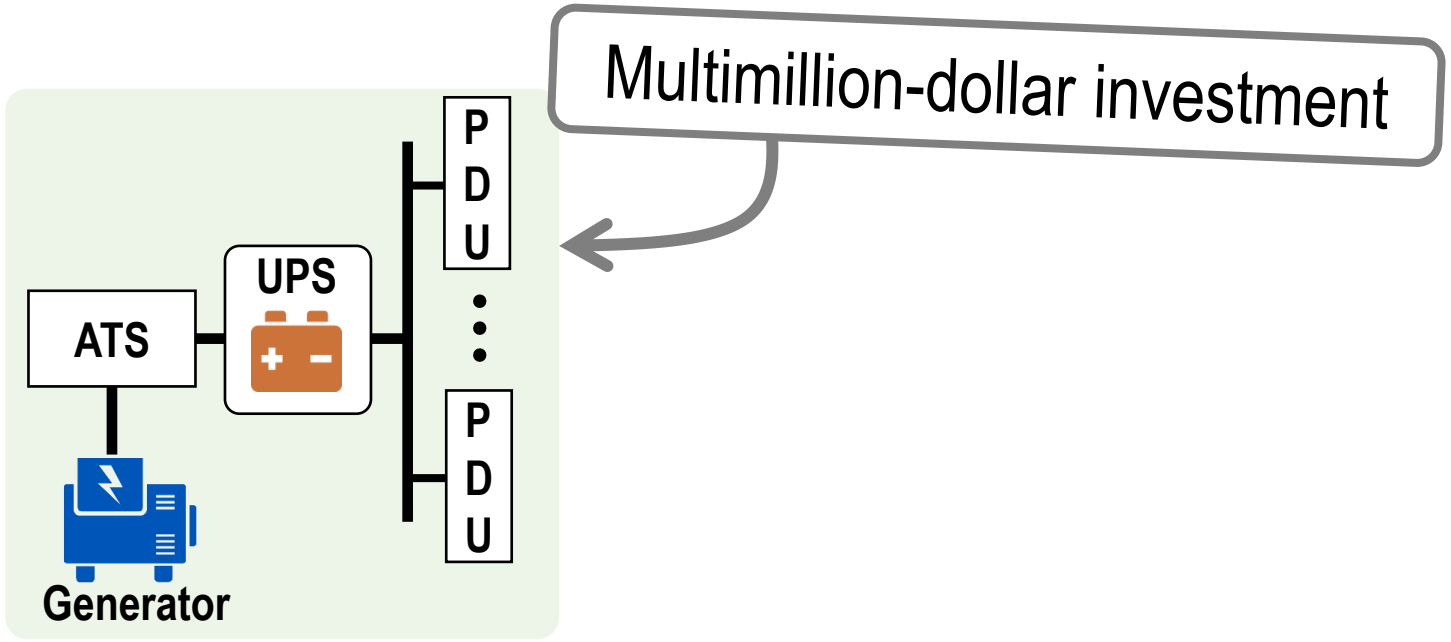
An overview of multi-tenant data center



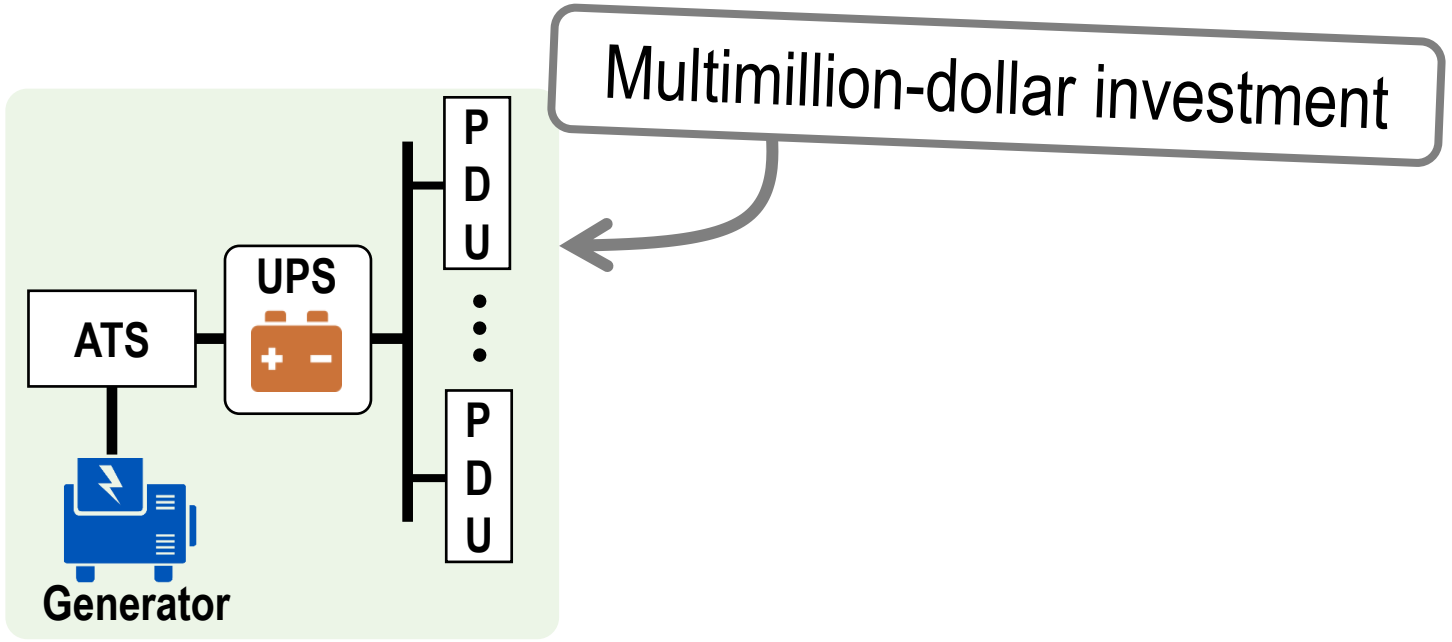
Securing the cyberspace

- DDoS attack, network intrusion, privacy protection, etc.

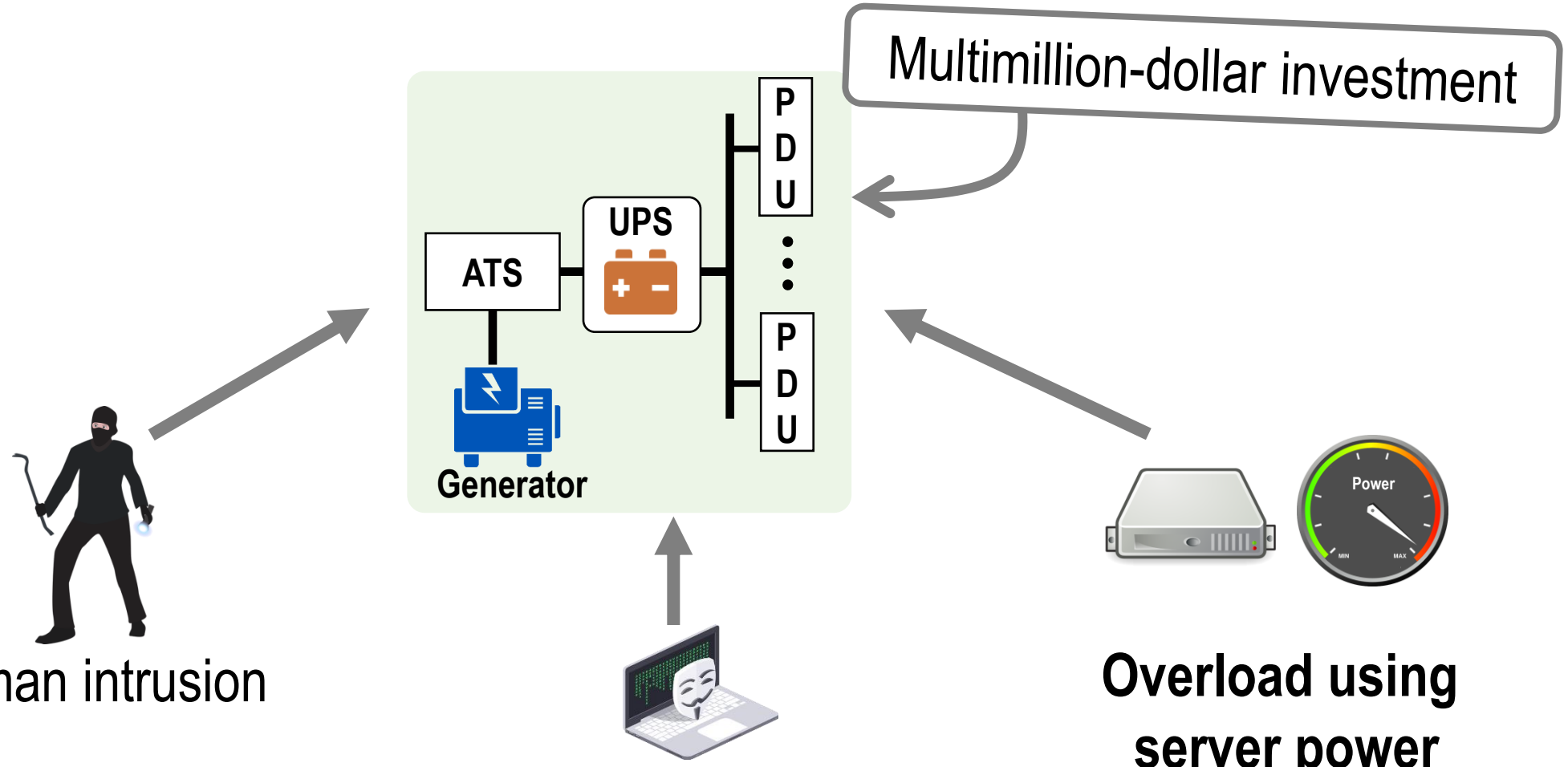
[Mirkovic, Sigcomm'04][Zhang CCS'12][Moon CCS'15][Dong CCS'17]…


Multimillion-dollar investment
ATS
UPS
PDU
PDU
Generator

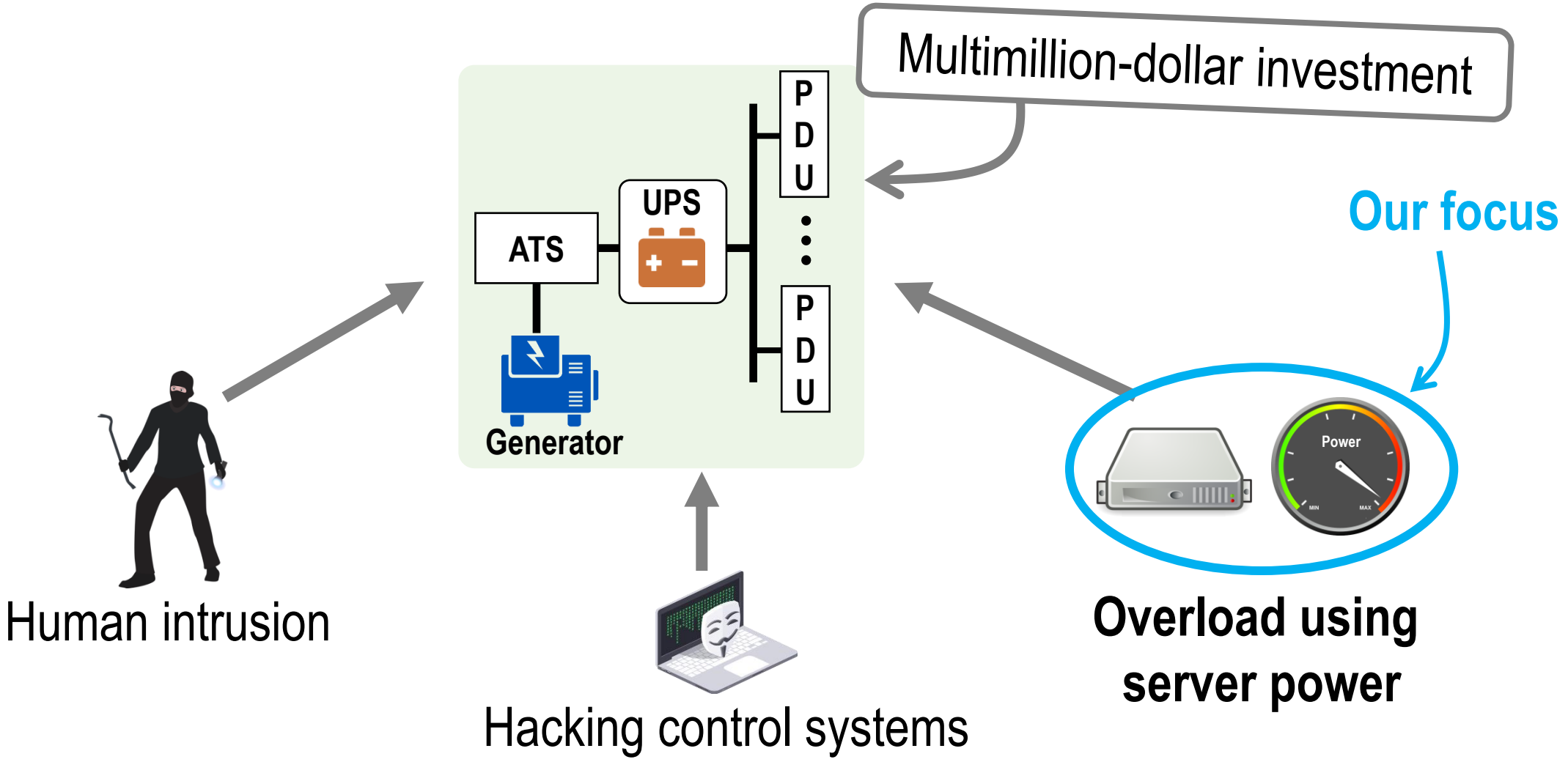
How to attack the physical infrastructure?

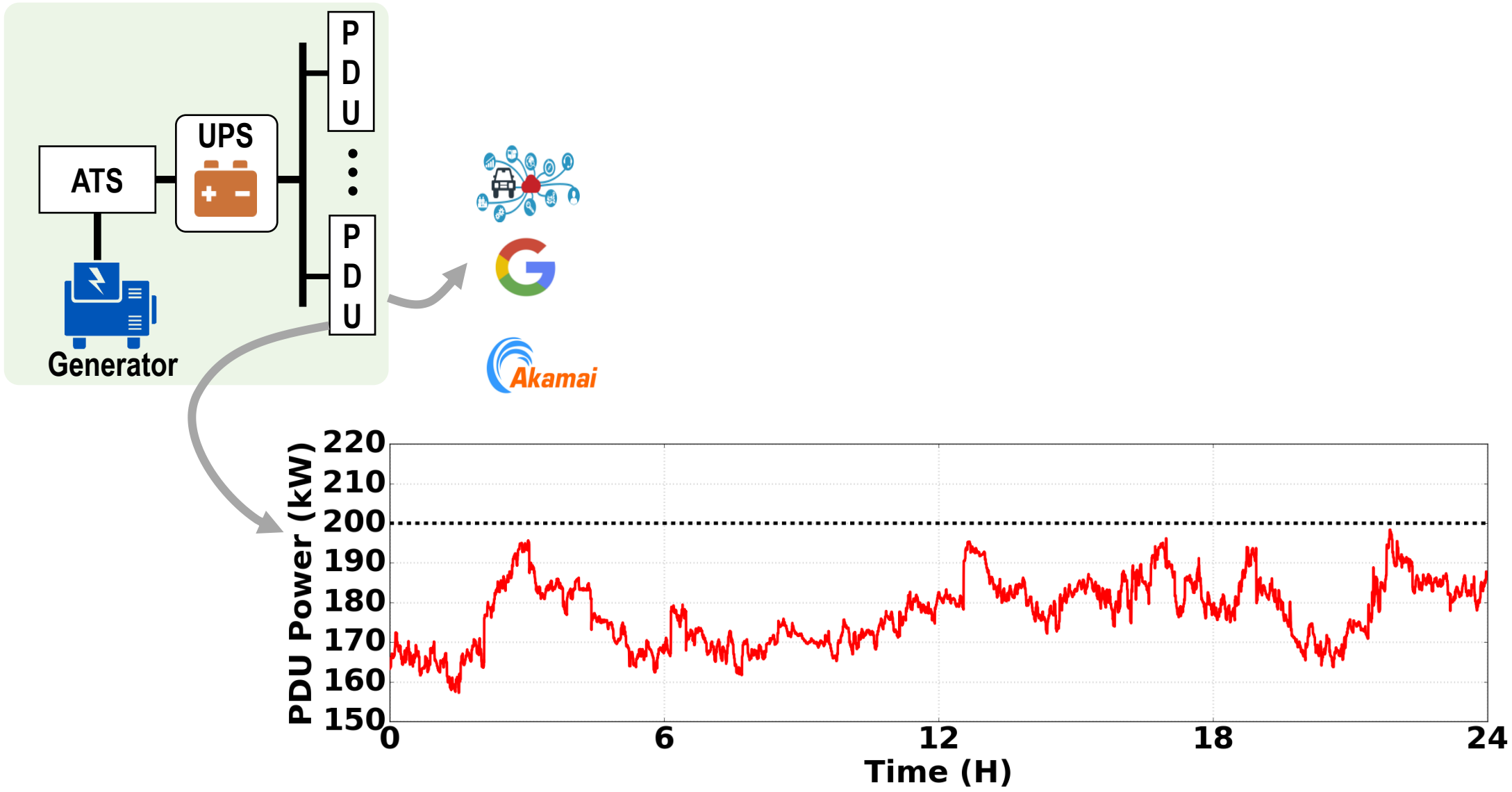


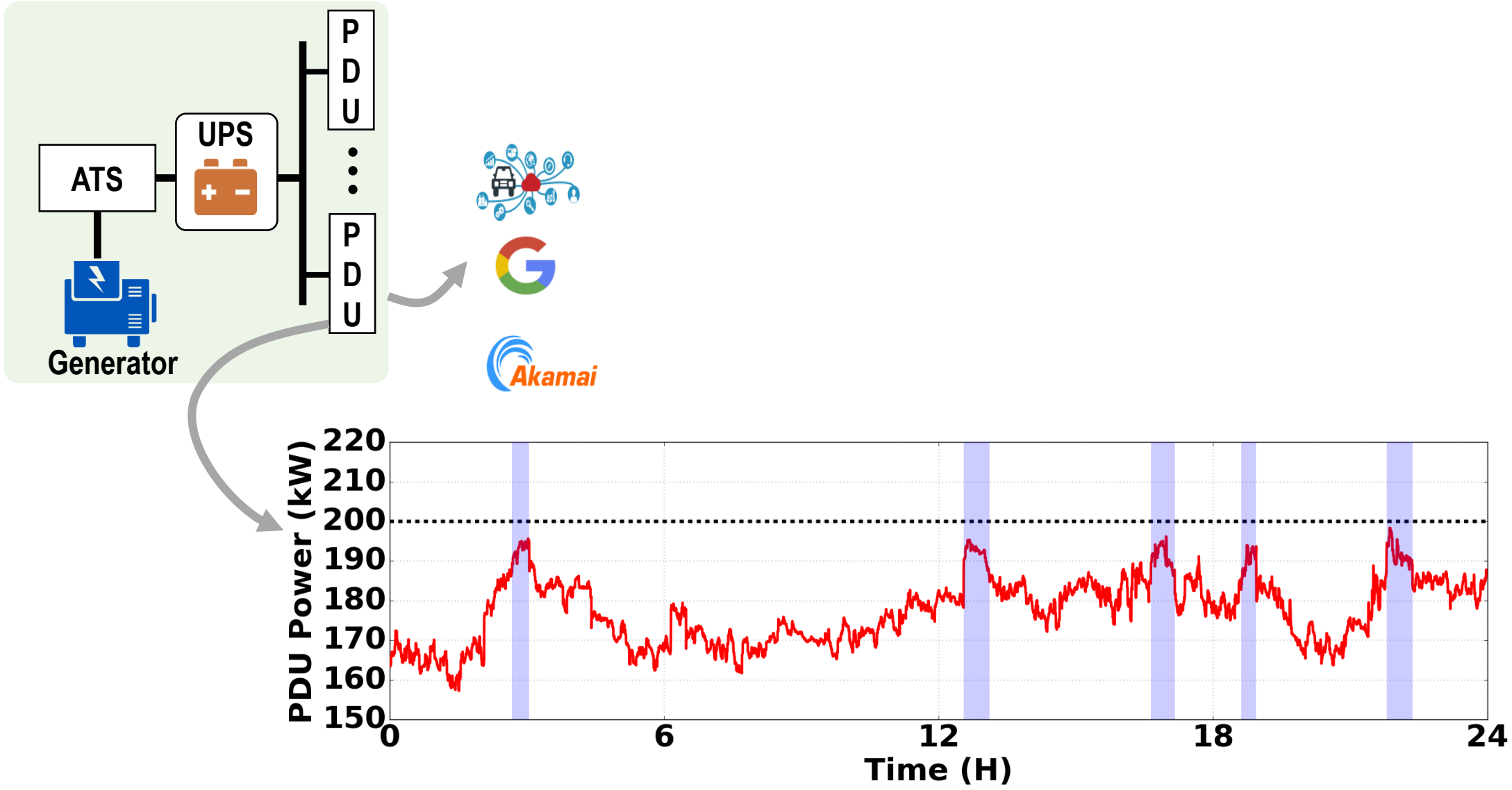
How to attack the physical infrastructure?



How to attack the physical infrastructure?

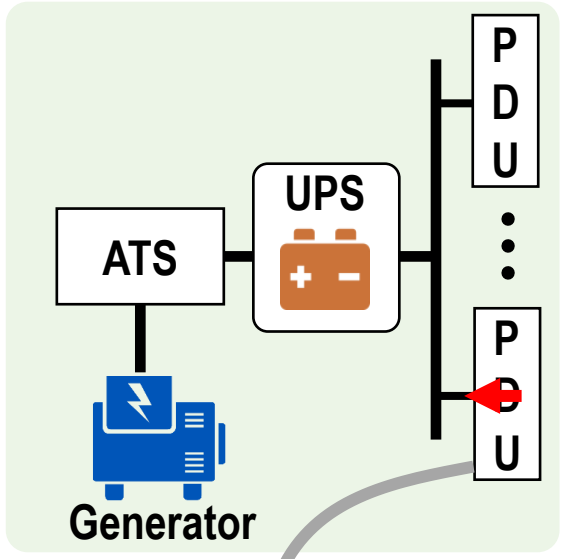



ATS
UPS
PDU
PDU
Generator
Akamai
PDU Power (kW)
220
210
200
190
180
170
160
150
0
6
12
18
24
Time (H)


ATS
UPS
PDU
PDU
Generator
Akamai
PDU Power (kW)
220
210
200
190
180
170
160
150
0
6
12
18
24
Time (H)

Power attack:

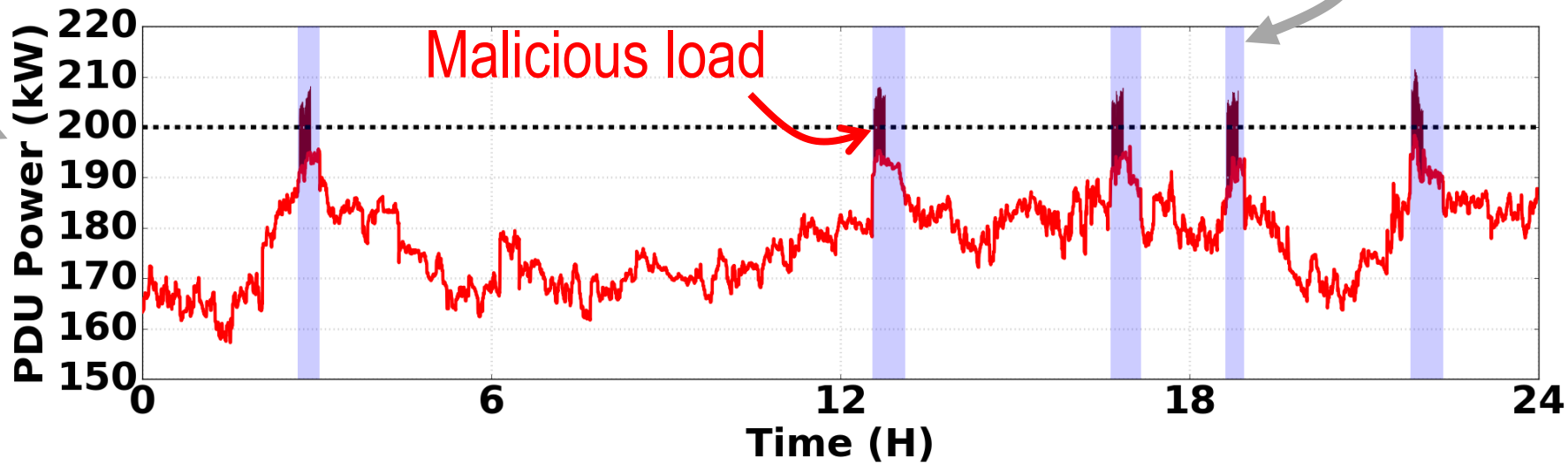
Well-timed power injection to overload the shared data center capacity, subject to all applicable usage constraints set by the operator



Malicious Tenant

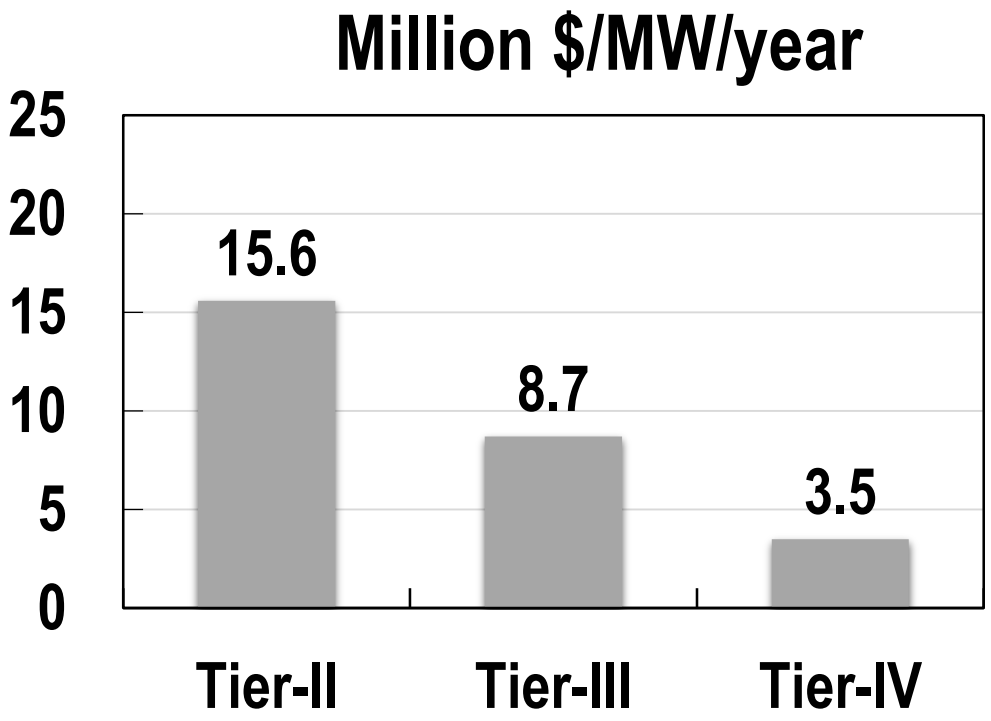
Akamai

Frequent capacity overloads…



Cost analysis

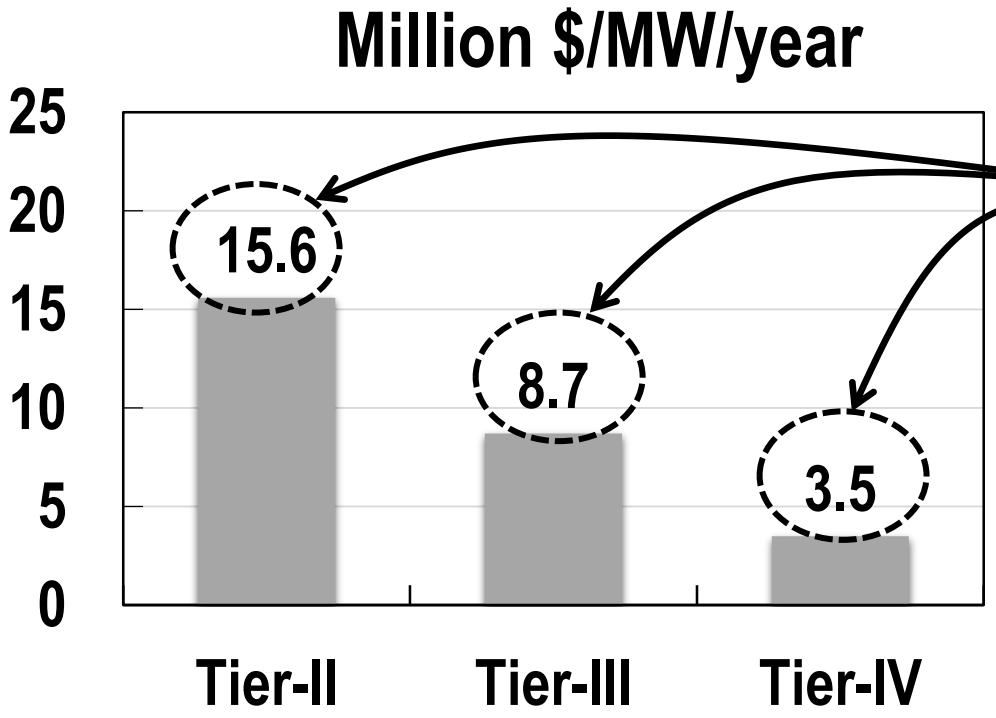
More likely to have an outage during overloads (e.g., risk increases by **~280 times** for a Tier-IV data center)



Estimated cost based on 5% overloads and a data center of 1MW-10,00sqft

Cost analysis

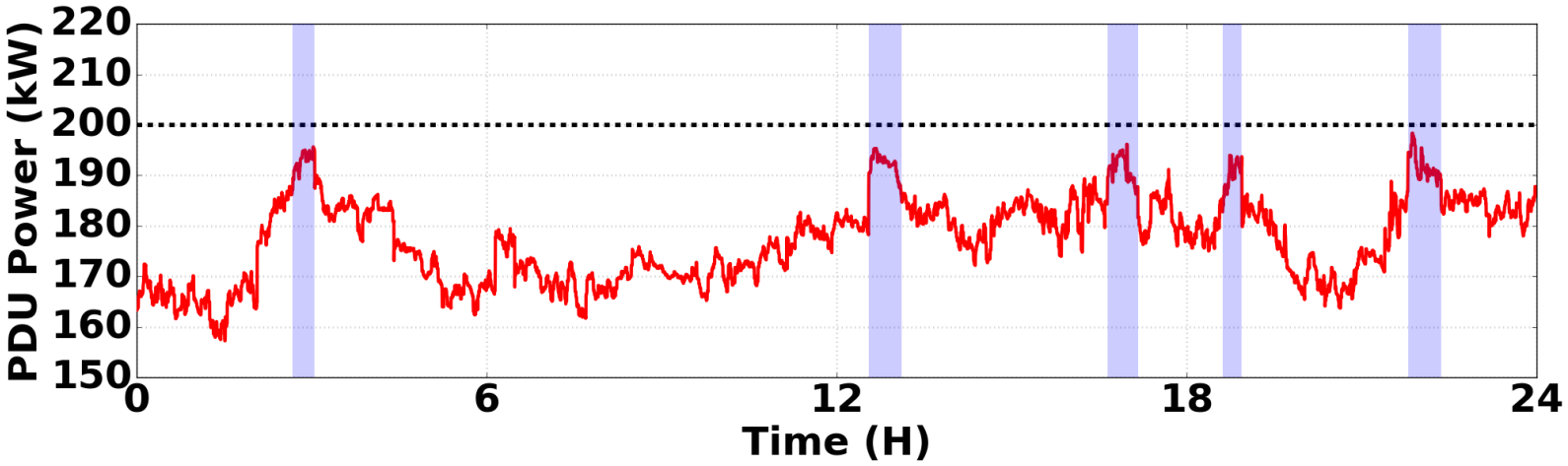
More likely to have an outage during overloads (e.g., risk increases by **~280 times** for a Tier-IV data center)



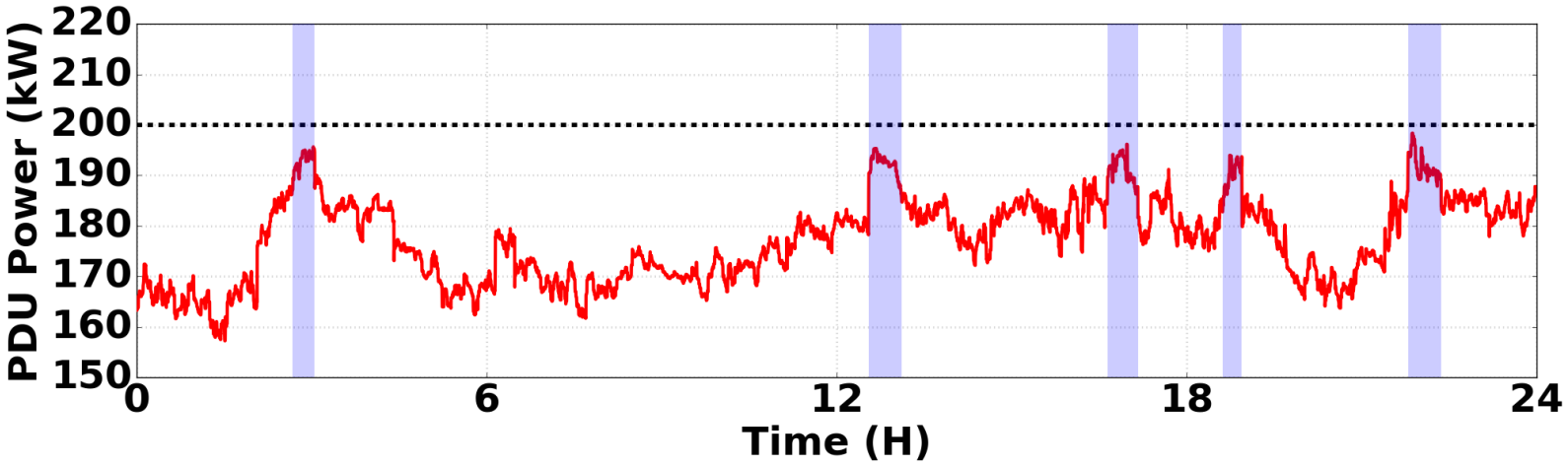
Annual cost > **$2 billion**
(if only 10% of the U.S. data centers are affected)

Estimated cost based on 5% overloads and a data center of 1MW-10,00sqft

How to precisely time power attacks?

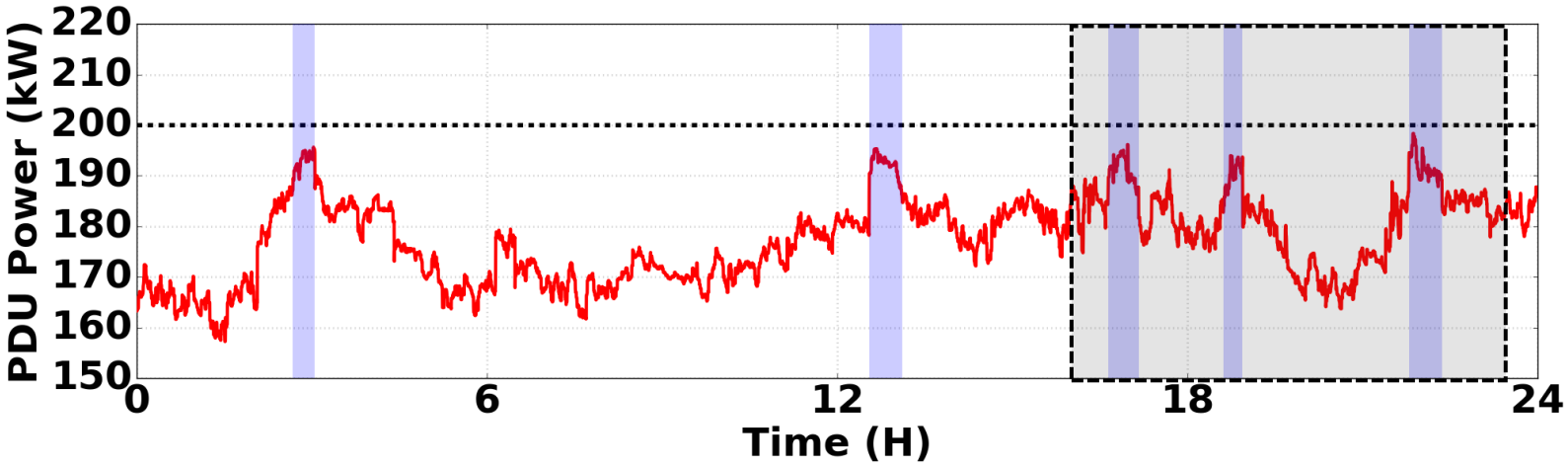


How to precisely time power attacks?



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

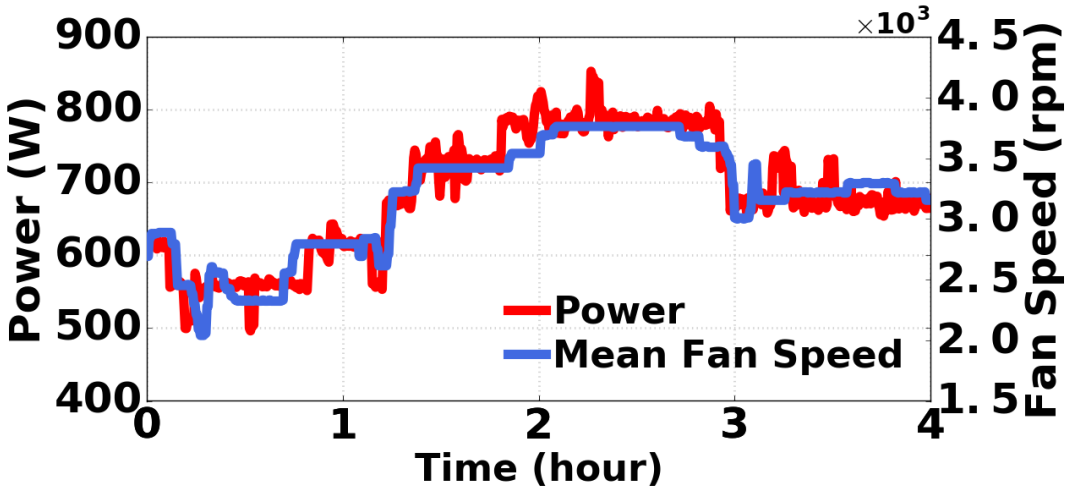
How to precisely time power attacks?



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

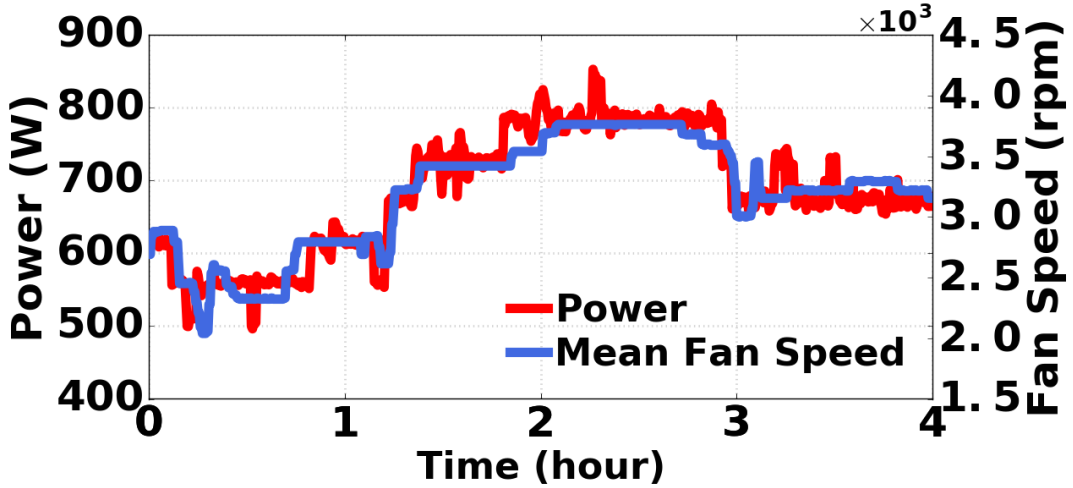
Server power → Heat → Cold Airflow → Fan Speed → Noise

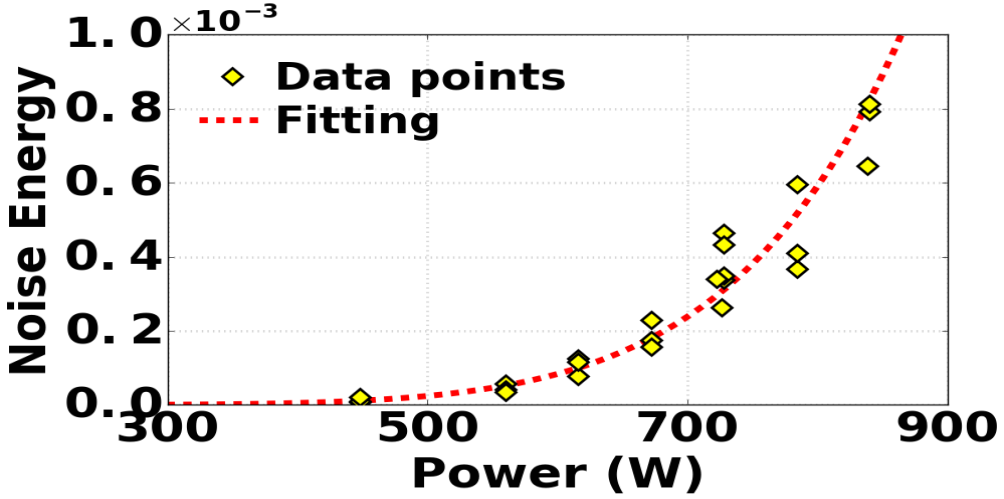
Dell PowerEdge servers



Server power → Heat → Cold Airflow → Fan Speed → Noise

Dell PowerEdge servers

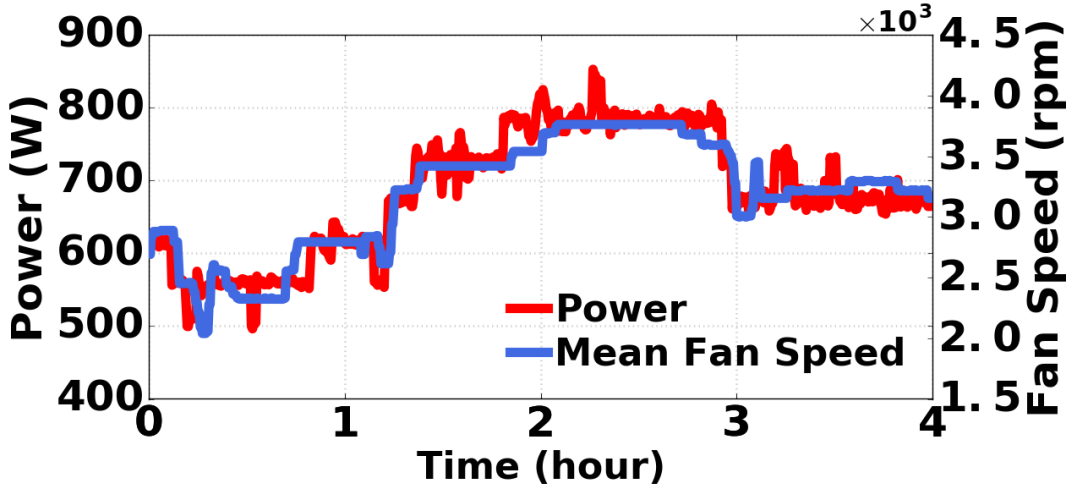


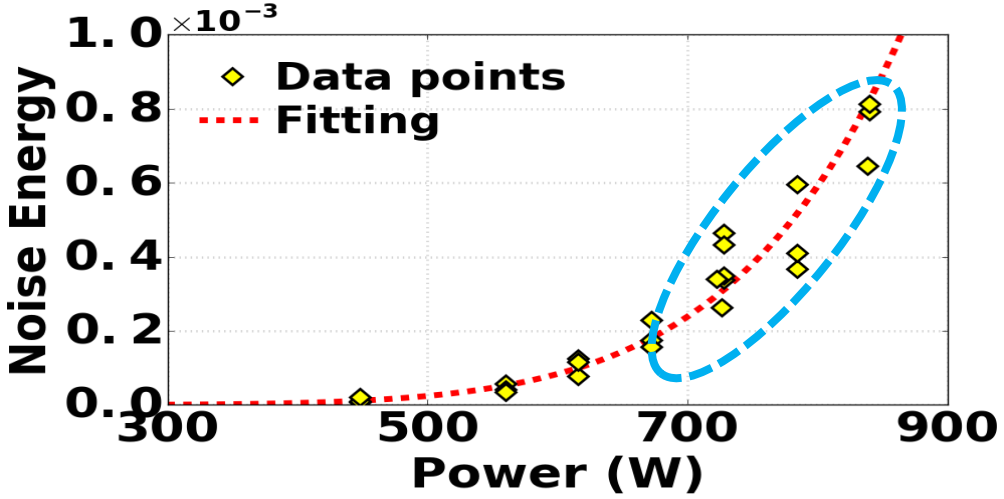


~~Server power → Heat → Cold Airflow → Fan Speed → Noise~~

An acoustic side channel…

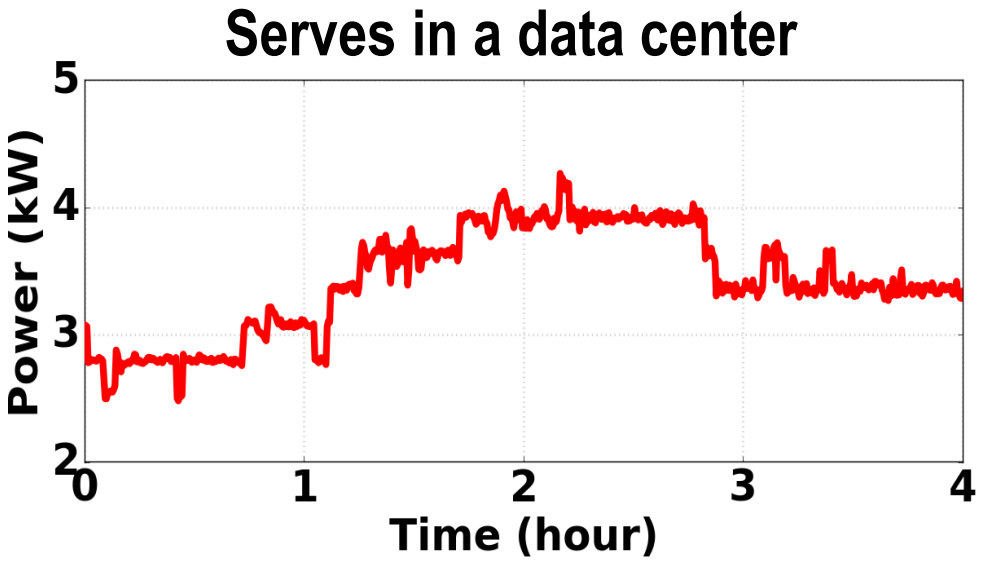
Dell PowerEdge servers

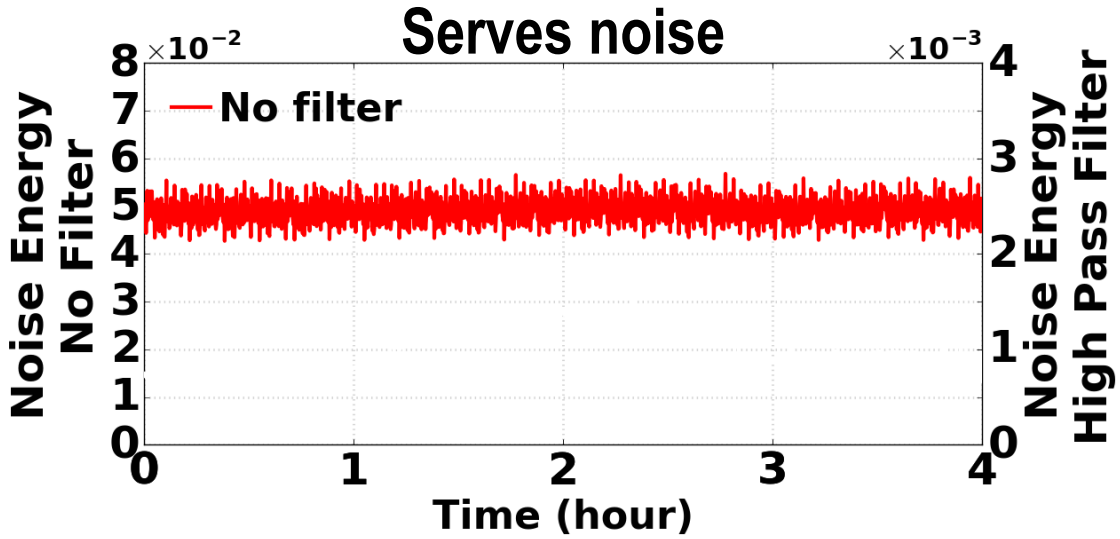




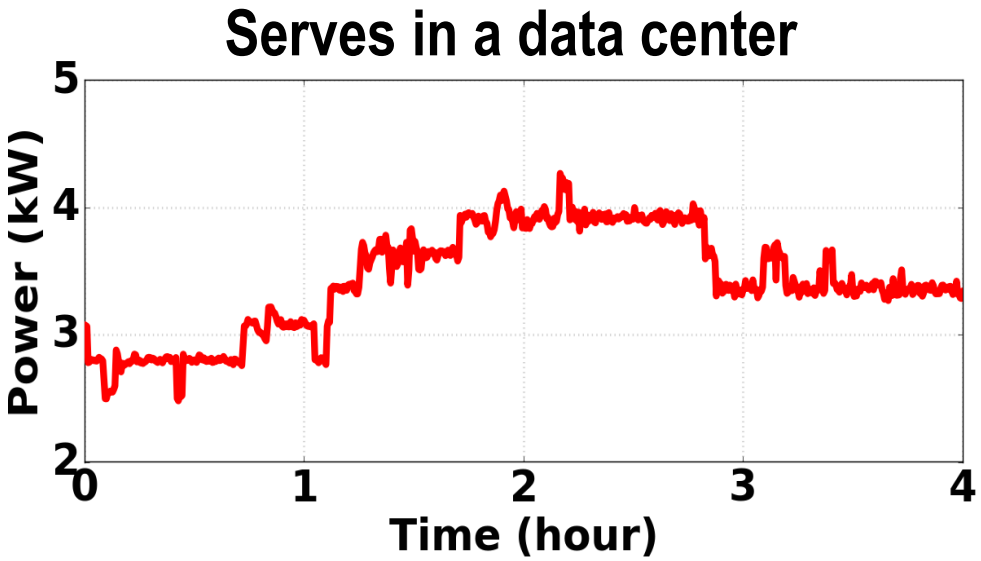
There are challenges…!

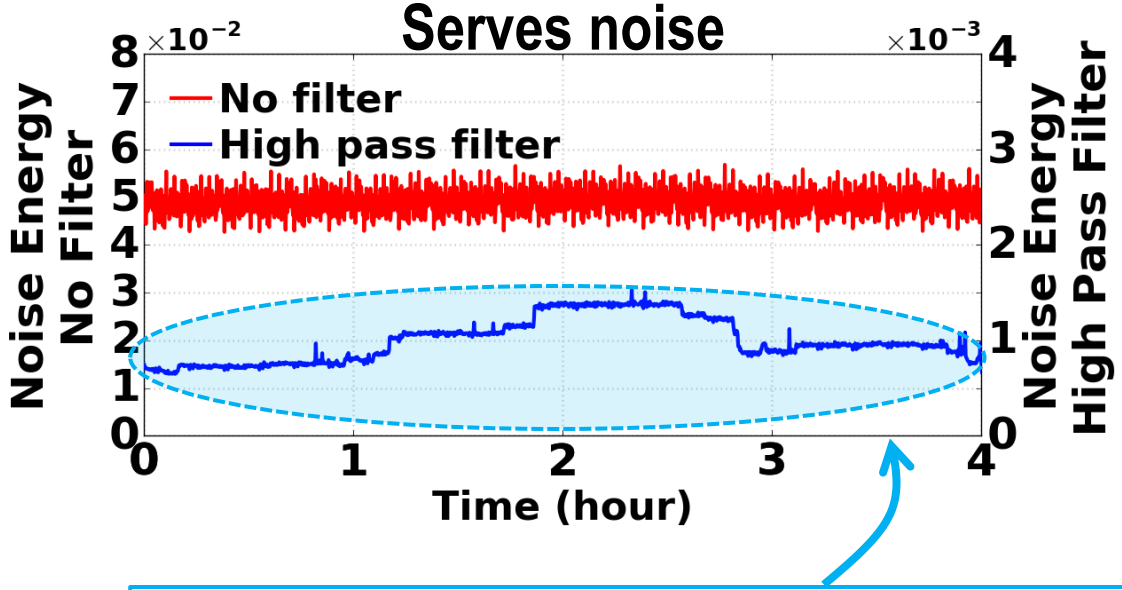
Suppressing the loud AC noise





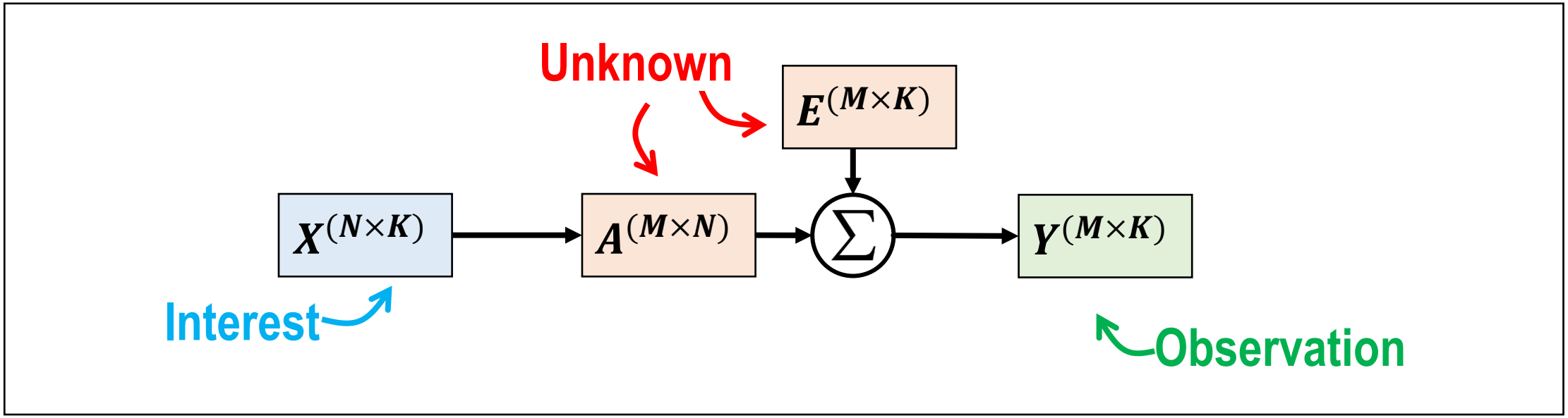
Suppressing the loud AC noise

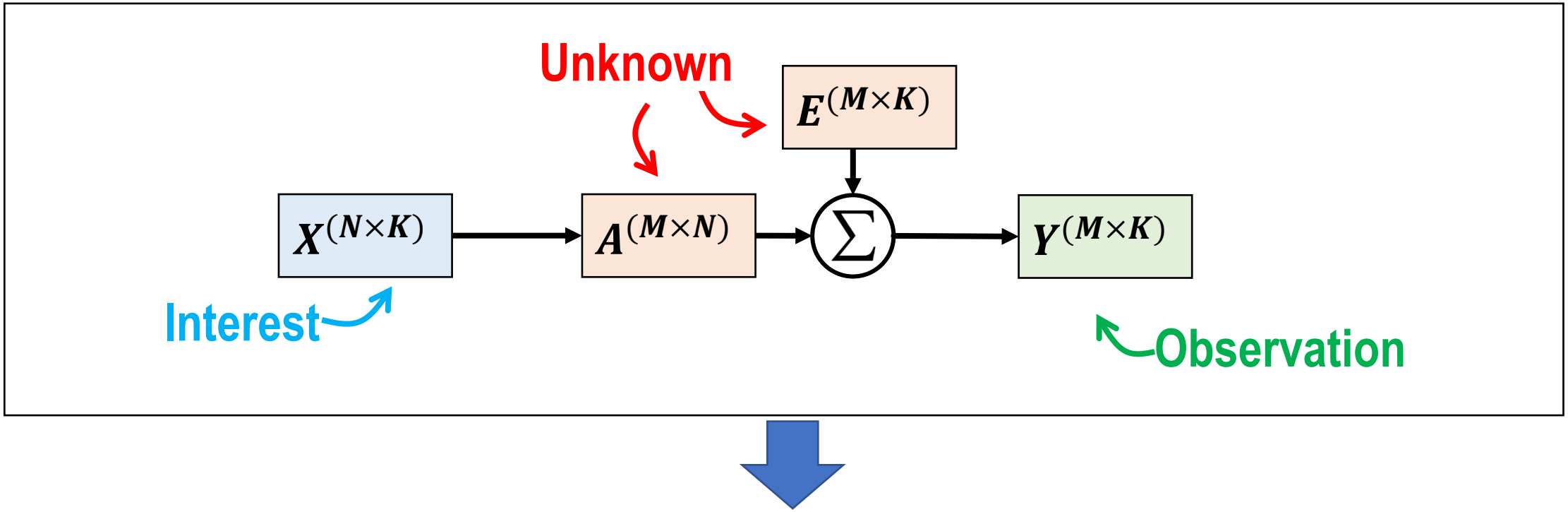




Noise from AC
<200Hz

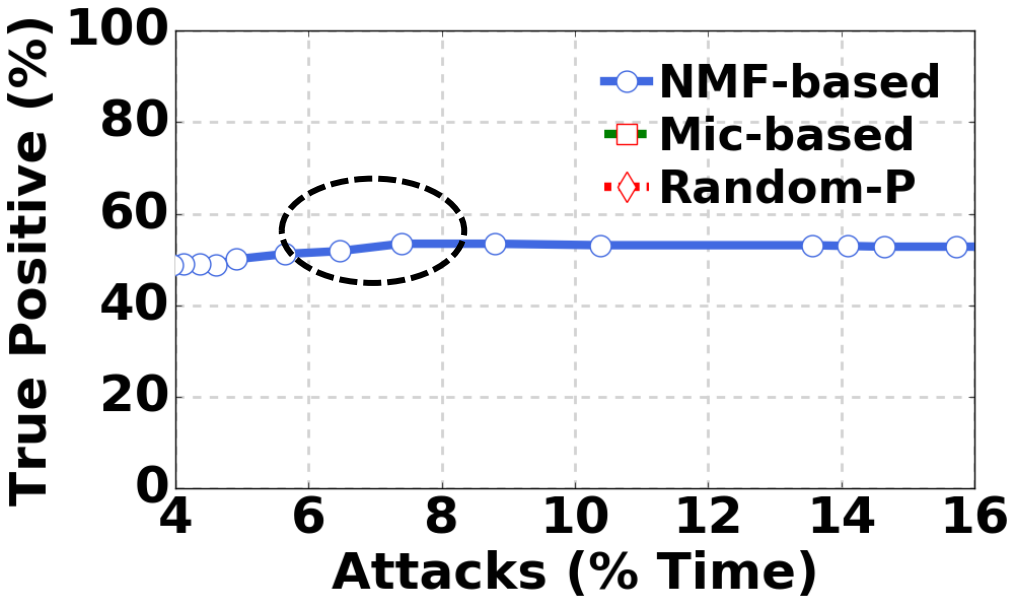
A high-pass filter reveals the server noise pattern

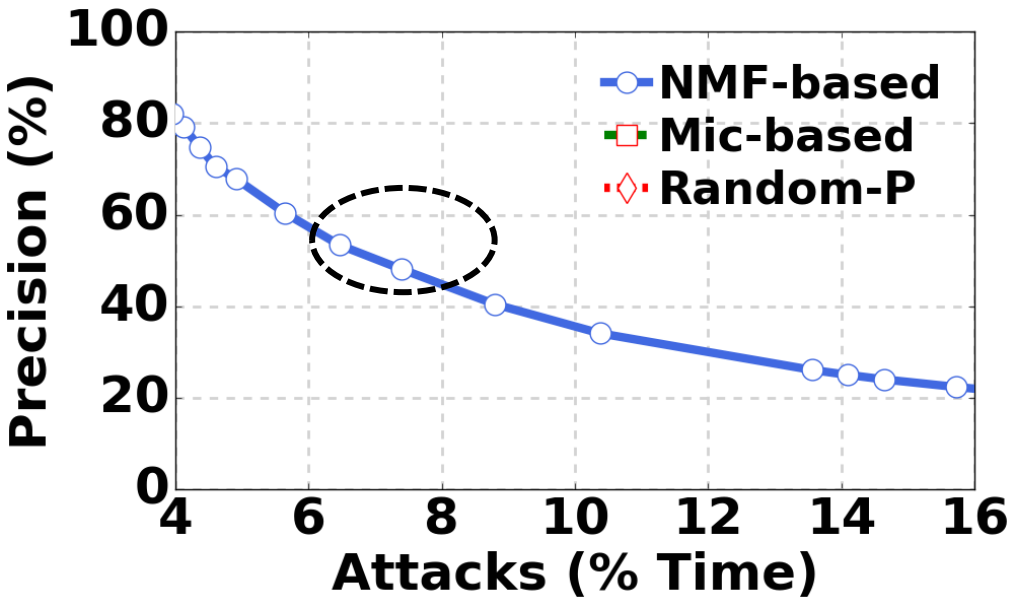

Unknown
$E^{(M\times K)}$
$X^{(N\times K)}$
$A^{(M\times N)}$
$\sum$
$Y^{(M\times K)}$
Interest
Observation



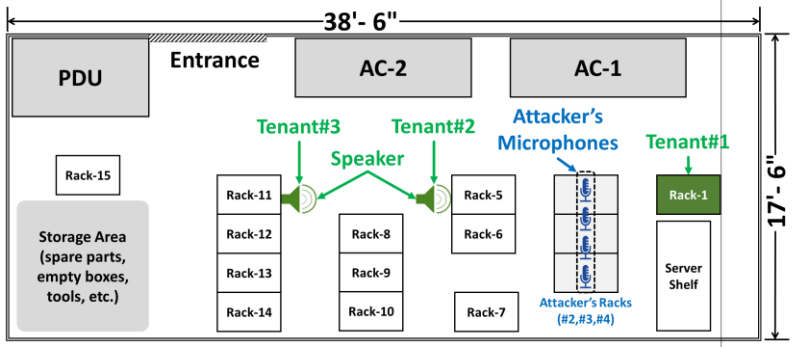
Solution: Blind source separation using non-negative matrix factorization (NMF)

Experimental evaluation

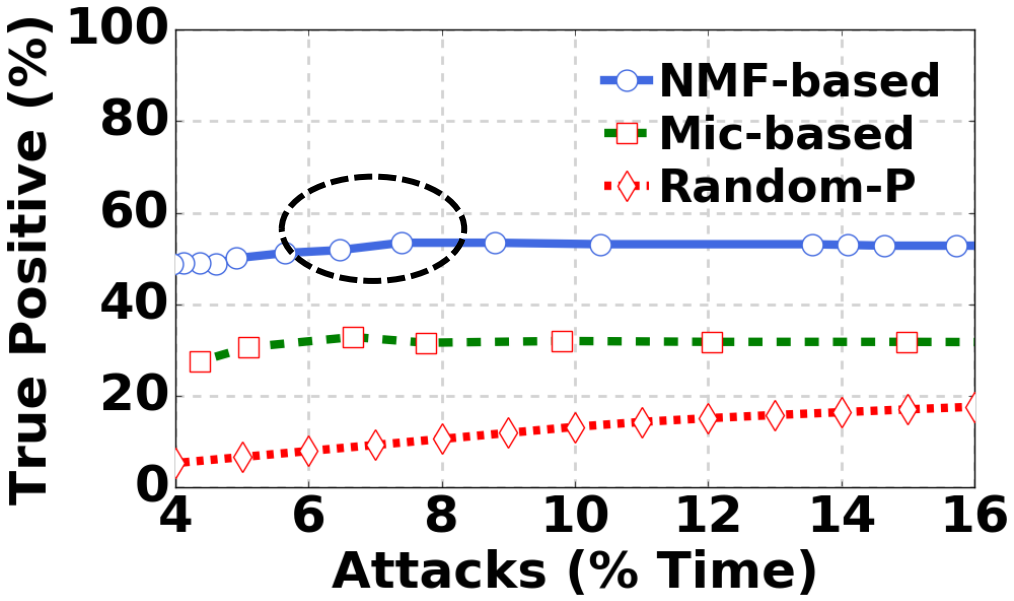


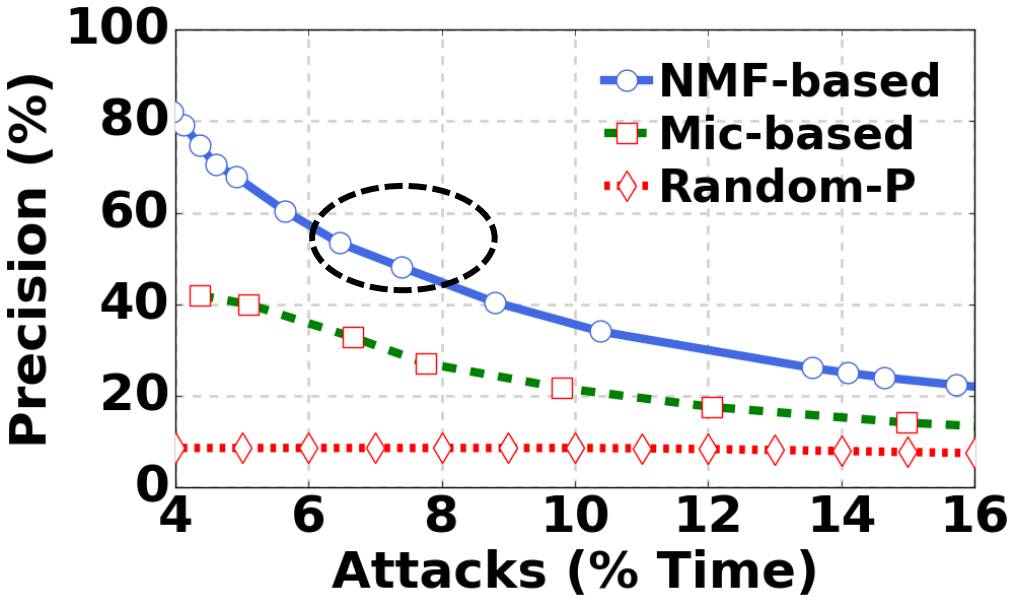


- Experimental settings
  - Run real workload traces in a university data center
- True positive: % of attack opportunities detected
- Precision: % of an attack being successful

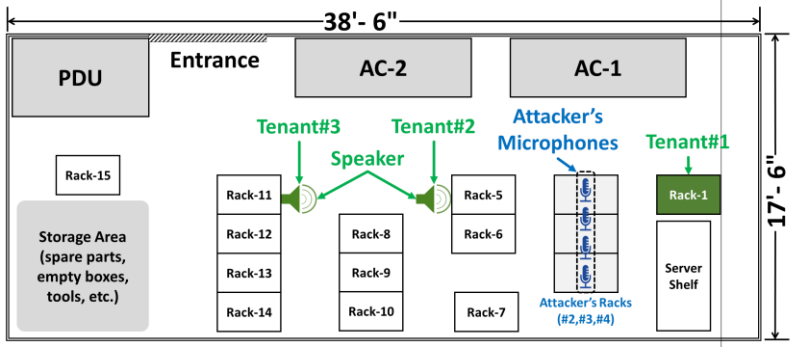


Experimental evaluation



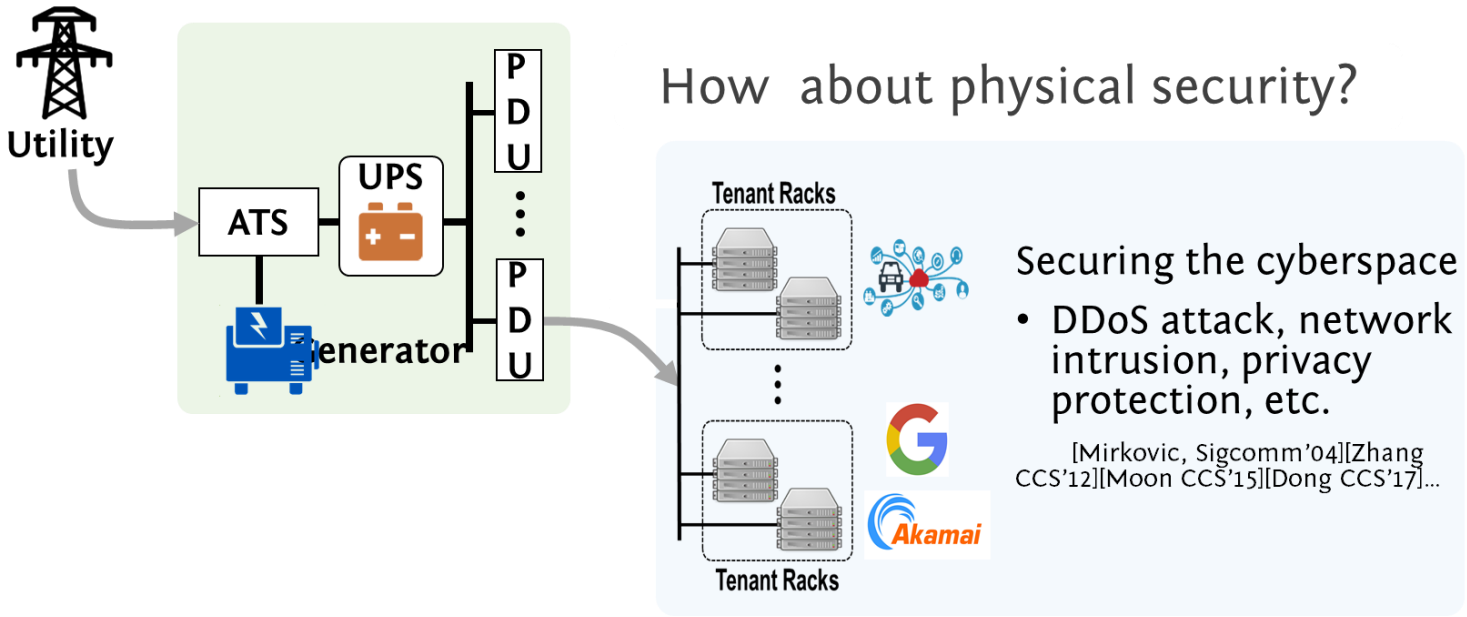


- Experimental settings
  - Run real workload traces in a university data center
- True positive: % of attack opportunities detected
- Precision: % of an attack being successful



Physical co-residence and space sharing result in physical side channels

Can be exploited to compromise data center physical security!



Thanks!