NYU TANDON SCHOOL OF ENGINEERING

Demand-Side Cybersecurity of Smart Grids

Samrat Acharya, Ramesh Karri, and Yury Dvorkin

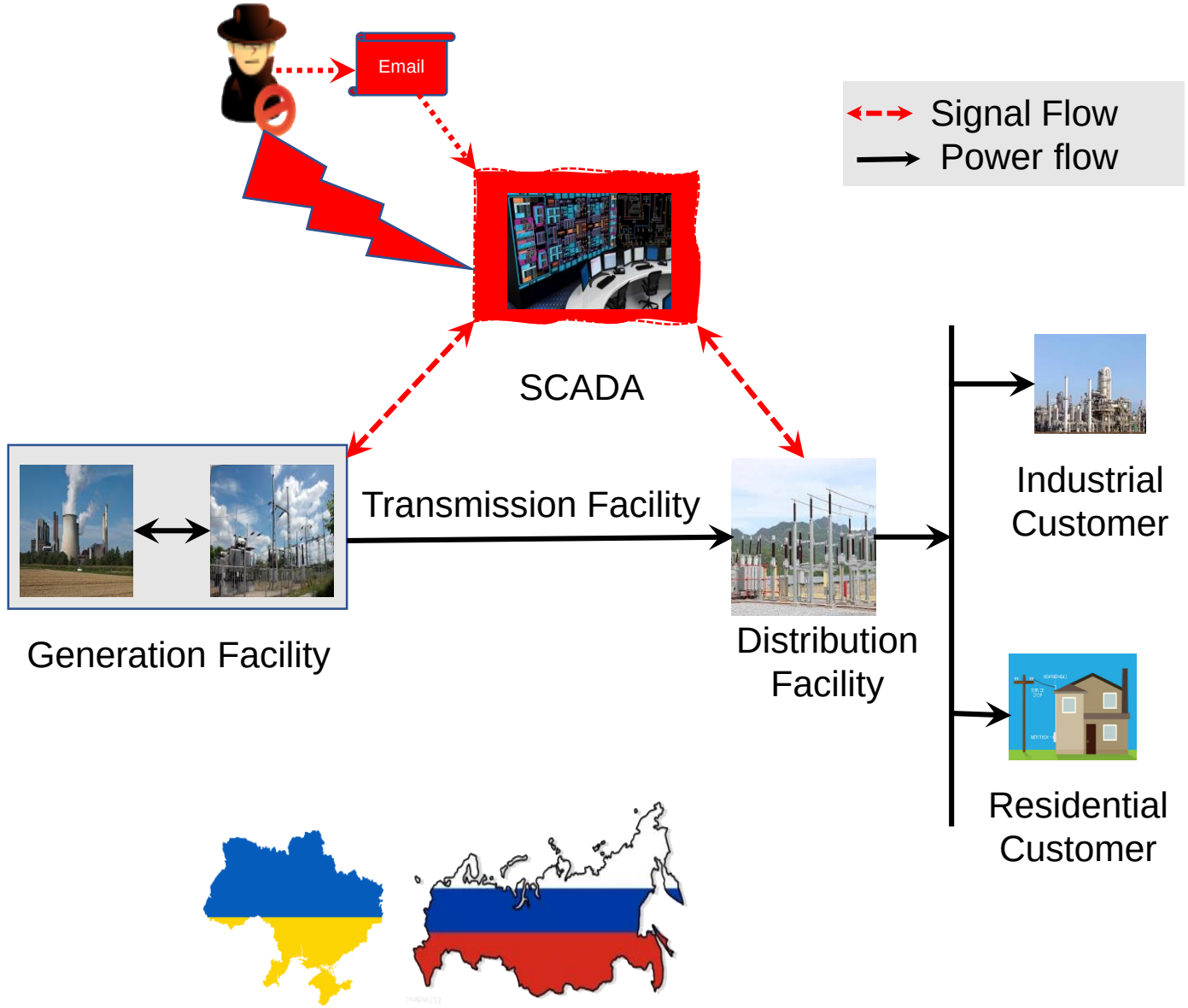
NSF

NYU Center for Cybersecurity

NYU CUSP
CENTER FOR URBAN SCIENCE+PROGRESS

Grid-Side Cyberattack

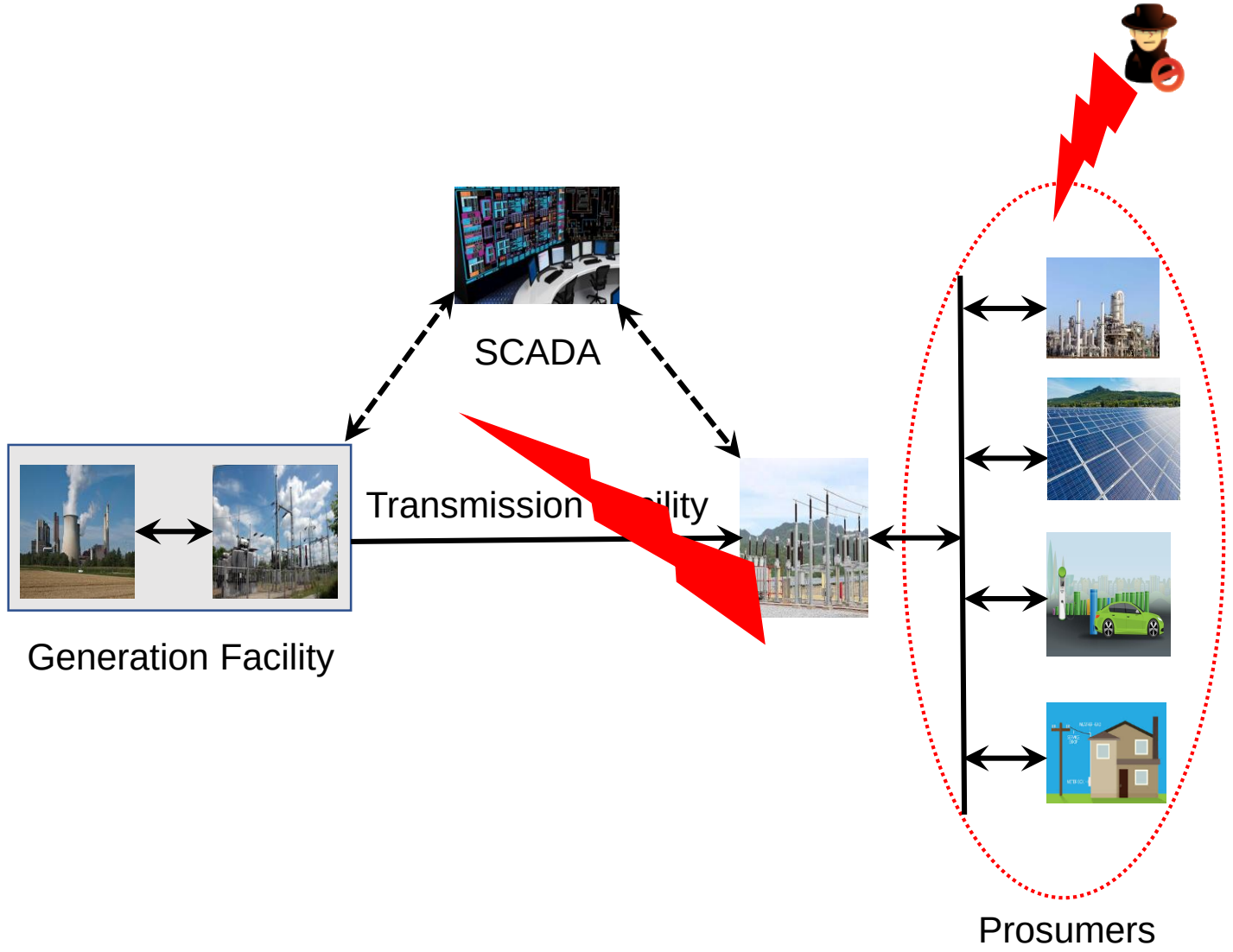
- Traditional Grids:
  - Unidirectional Power Flow
  - Centralized SCADA control
- Grid-Side Attacks:
  - SCADA (2015 Ukraine Power Grid Attack)
  - Expertise and resources required to break industry-grade defense.



Demand-Side Cyberattack

NYU TANDON SCHOOL OF ENGINEERING

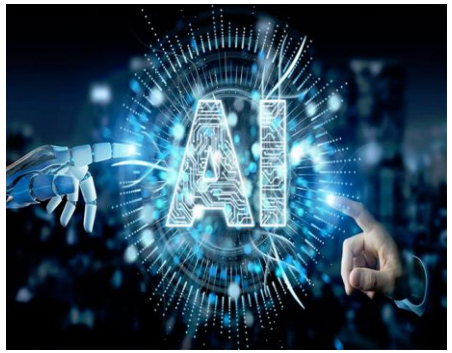
- Evolution of Smart Grids:
  - Decentralized Controllers
  - Bidirectional Power Flow
  - Customers to Prosumers
- Demand-Side Attacks:
  - Billions of IoT devices (~31 billions today, 75 billions by 2025)*
  - Customers poor cyber hygiene
  - 2016 Mirai botnet via IoT devices



* https://securitytoday.com/Articles/2020/01/13/The-IoT-Rundown-for-2020.aspx?Page=2

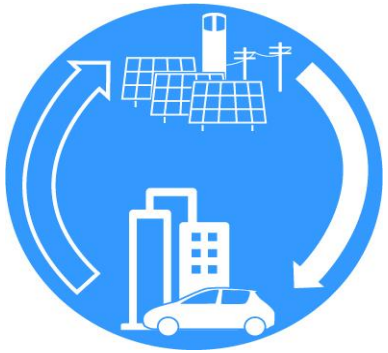
Demand-Side Attack Vectors

EV Charging



Artificial Intelligence (AI)

Public Data



Demand Response (DR)

Why Attackers target EV Charging?

1. Rapidly expanding numbers of EVs and EV charging stations (EVCSs)

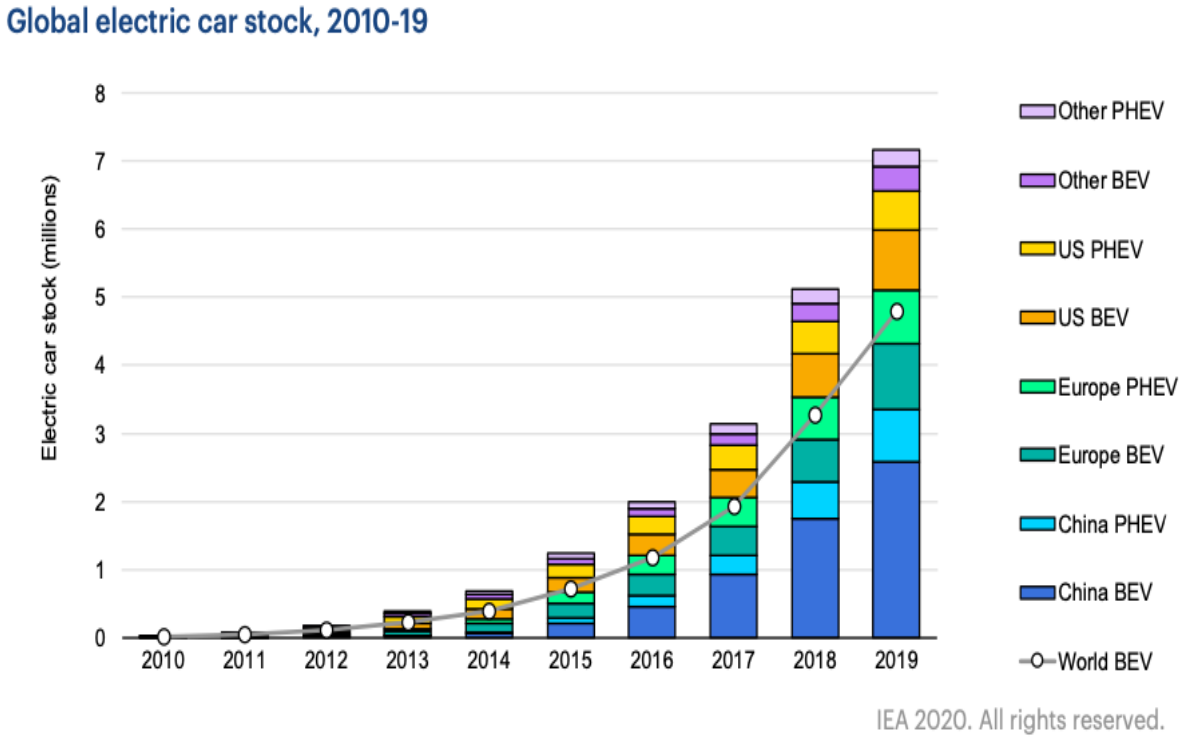


*Fig: Global electric car sales market share, 2013-19 **

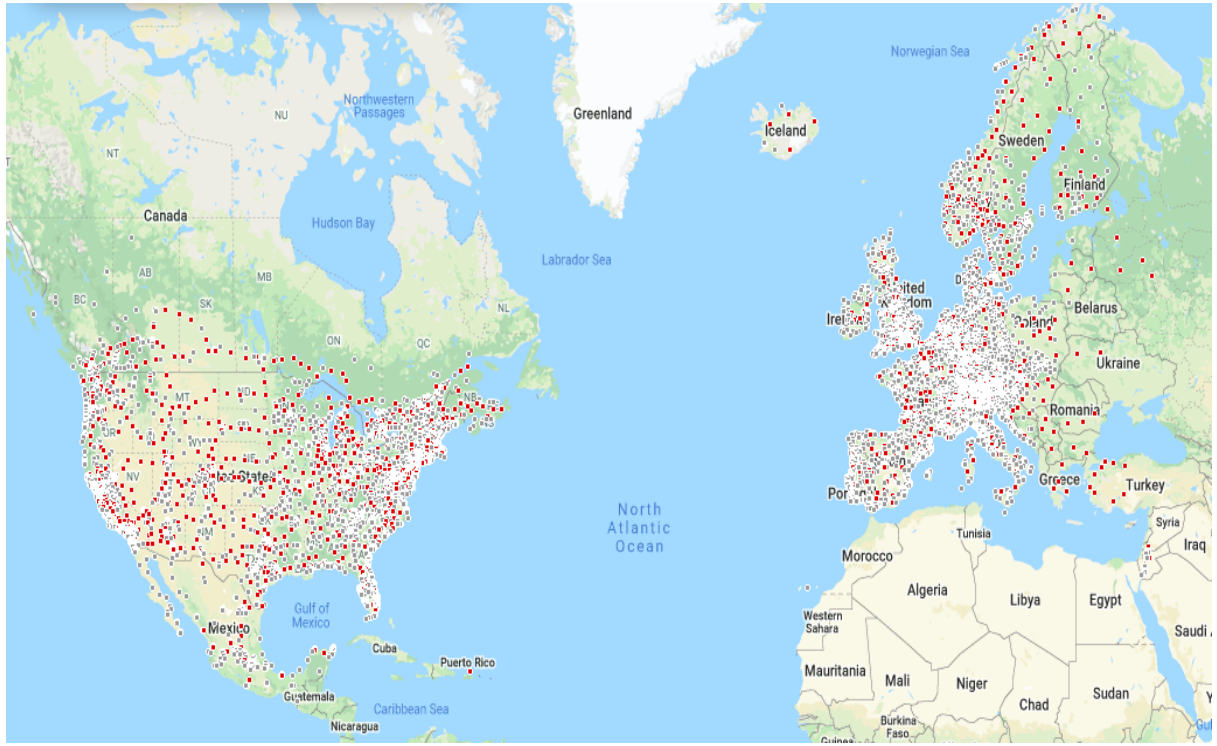


Fig: Tesla chargers

**Global EV Outlook 2019, IEA*

***Tesla Superchargers*

Why Attackers target EV Charging?

2. Growing capacity of EV and EVCSs

<3 kW AC

<20 kW AC

>350 kW DC

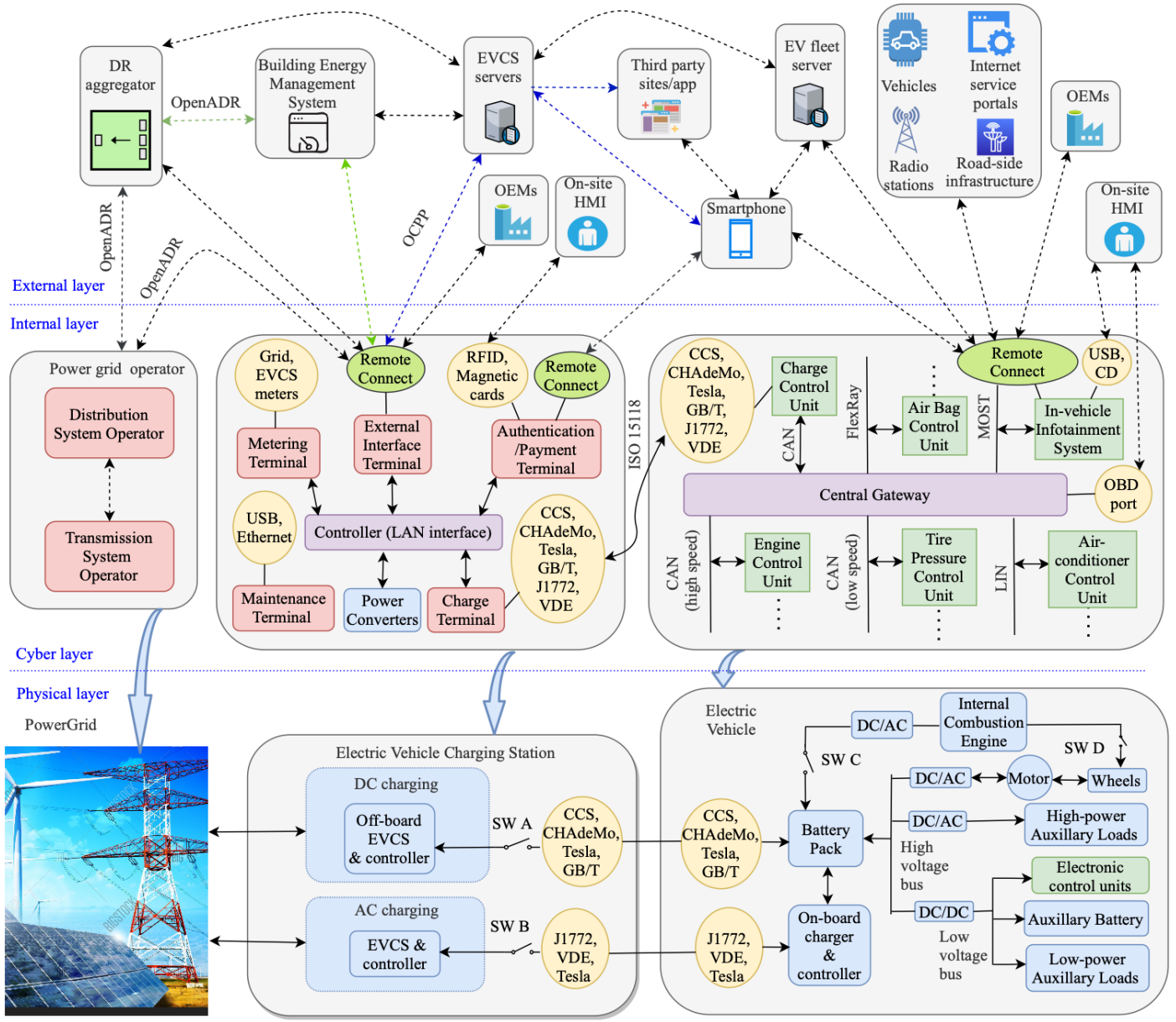
>100 kWh

100s of miles in a single charge of <30 minutes

3. Increasing internet-enabled charging

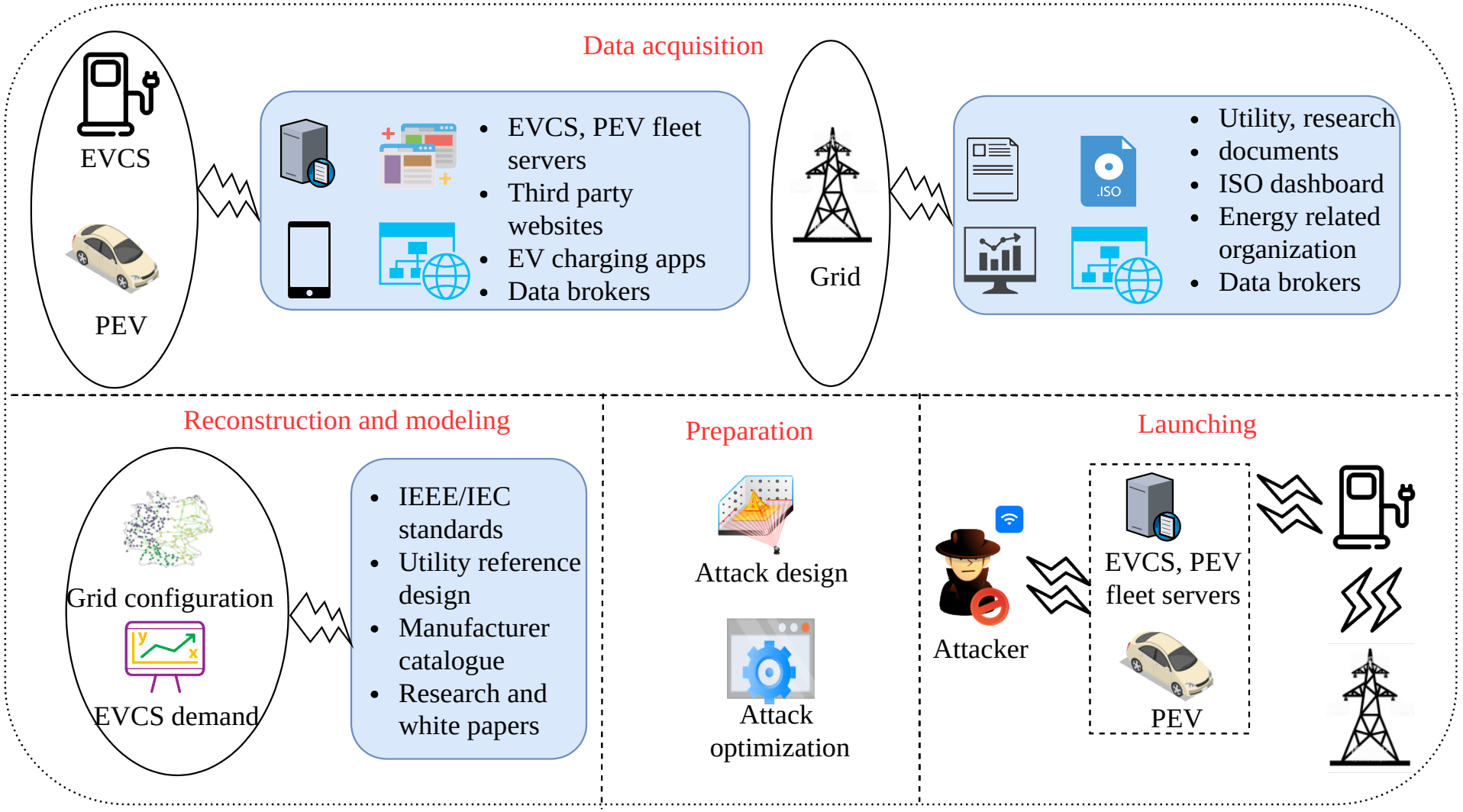
Cyber-Physical Outlook of EV Charging

- No or immature charging standards
- Third-party facilitating EV charging
- Public charging data



1. S. Acharya, Y. Dvorkin, and R. Karri, “Public plug-in electric vehicles + grid data: Is a new cyberattack vector viable ?” IEEE Transactions on Smart Grid, 2020.
2. S. Acharya, Y. Dvorkin, H. Pandˇzi ́c , and R. Karri, “Cybersecurity of Smart Electric Vehicle Charging” IEEE Access, 2020

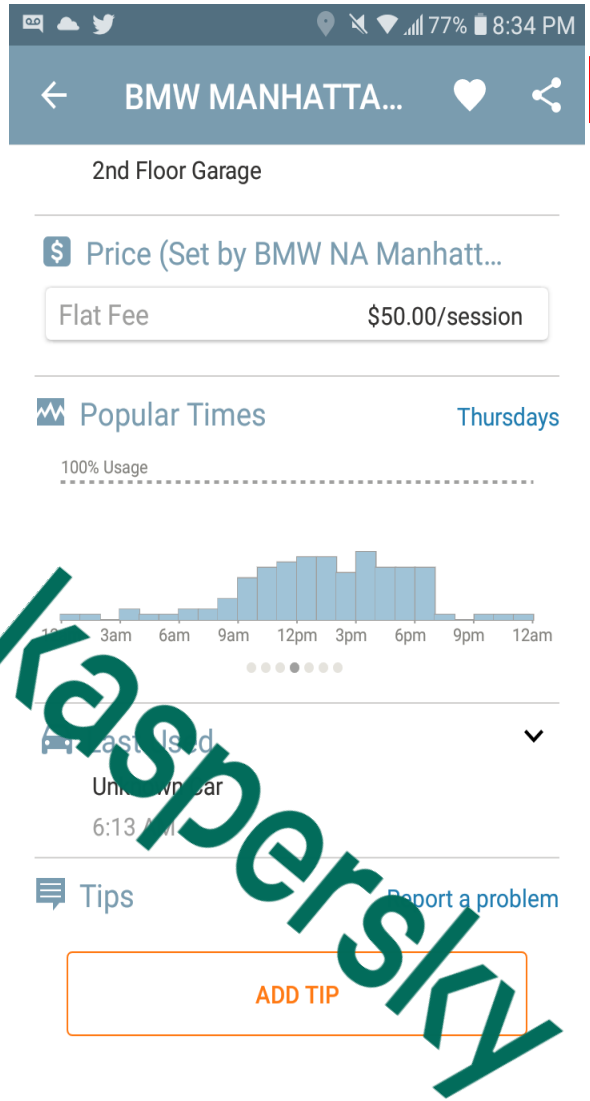
Attack Development Using EV + Public Data

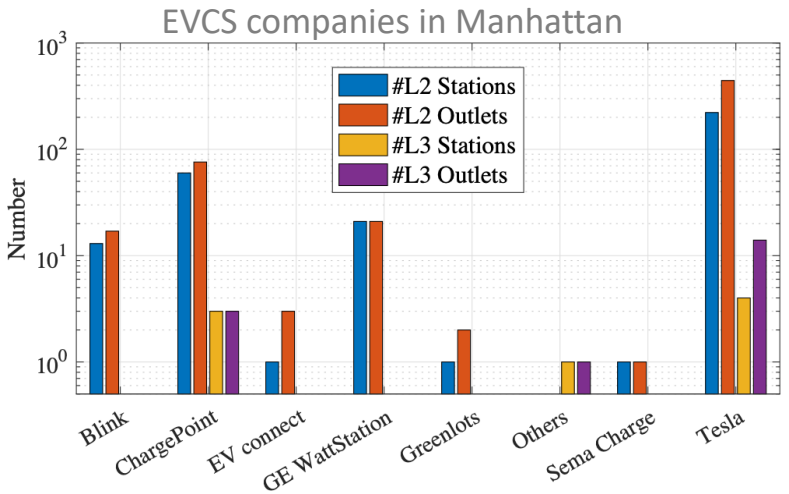


S. Acharya, Y. Dvorkin, and R. Karri, "Public plug-in electric vehicles + grid data: Is a new cyberattack vector viable?" IEEE Transactions on Smart Grid, 2020.

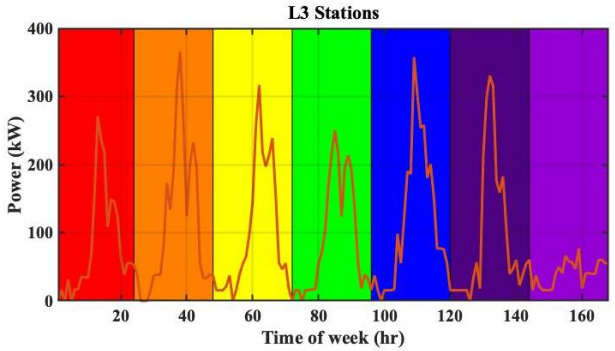
EV Charging Public Data: Manhattan Case

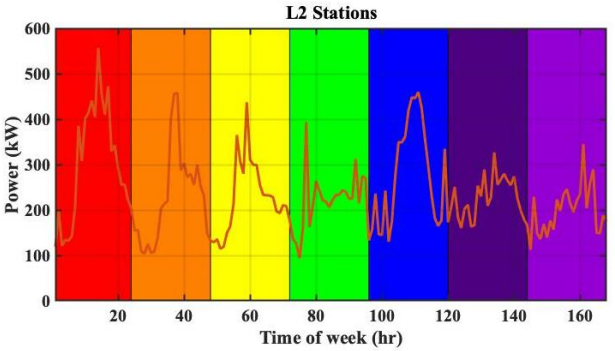
NYU TANDON SCHOOL OF ENGINEERING

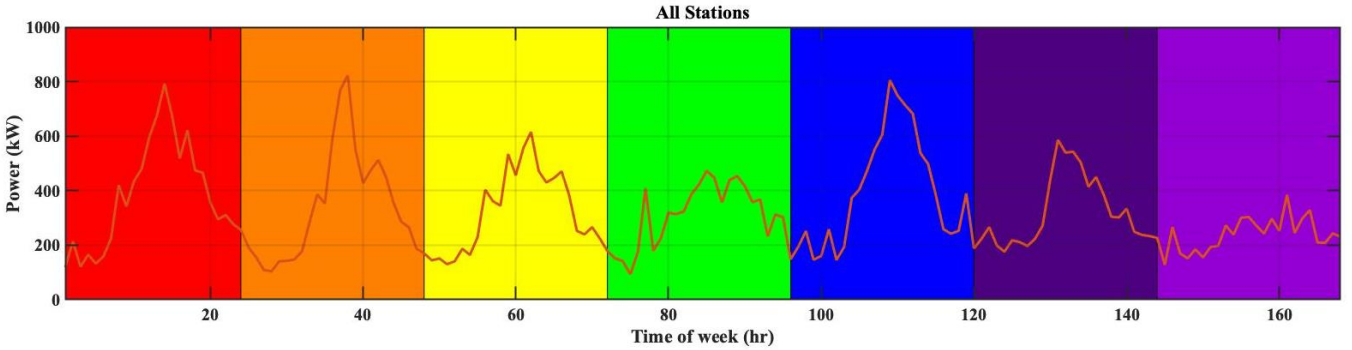




We got EV data!





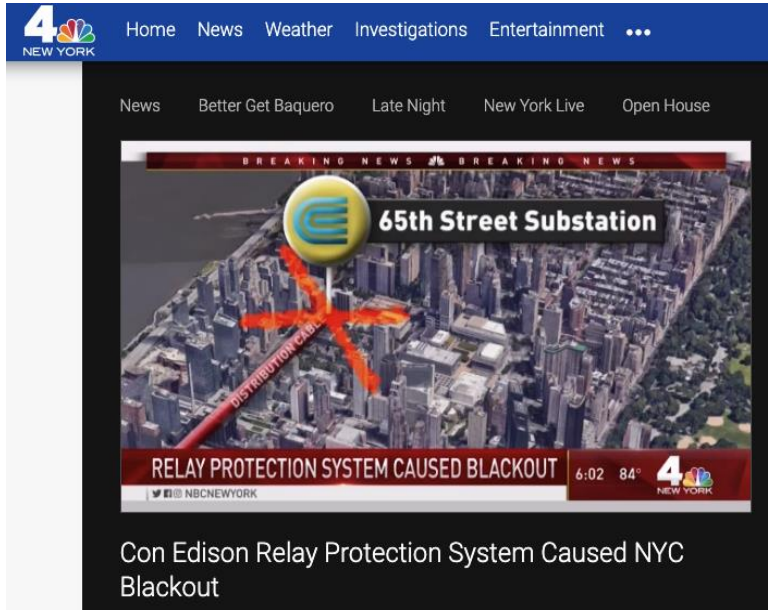


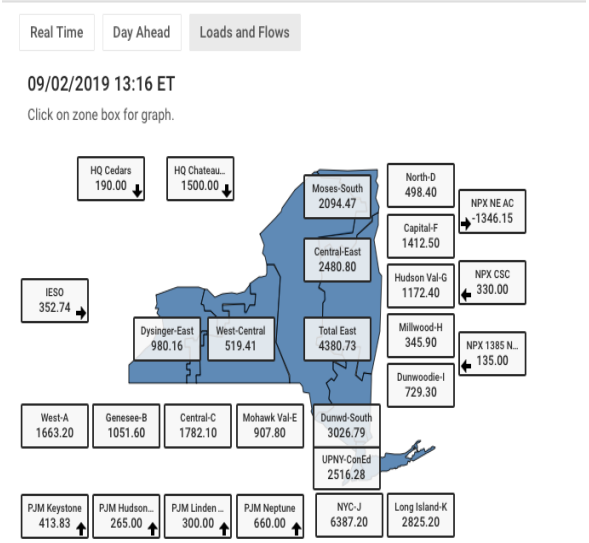
Public Power Grid Data: Manhattan Case

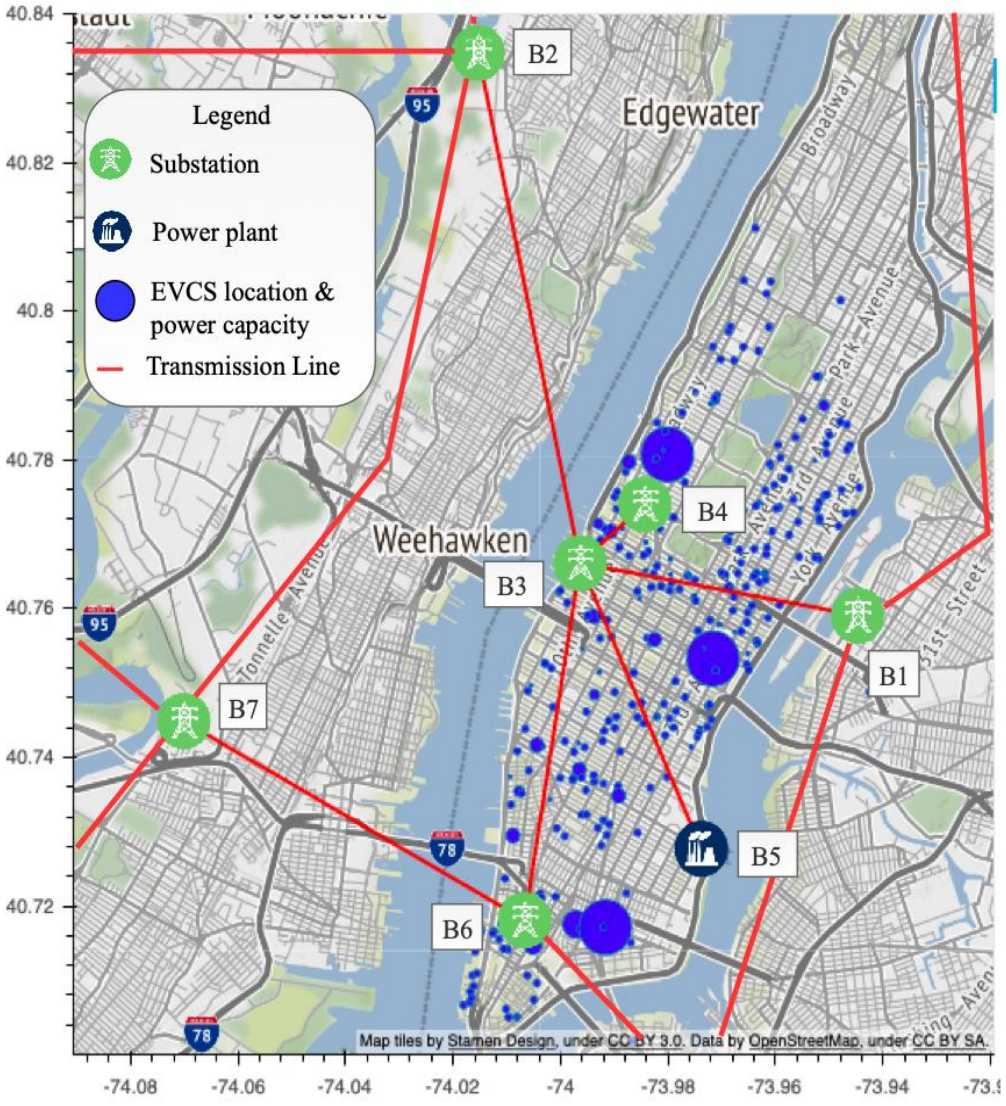
NYU TANDON SCHOOL OF ENGINEERING

Where Do We get Grid Data?

- Google Maps
- Con Edison
- New York Independent System Operator
- US Energy Information Administration
- Reports, public releases, news reporting, etc.







Reconstruction of Grid Layout

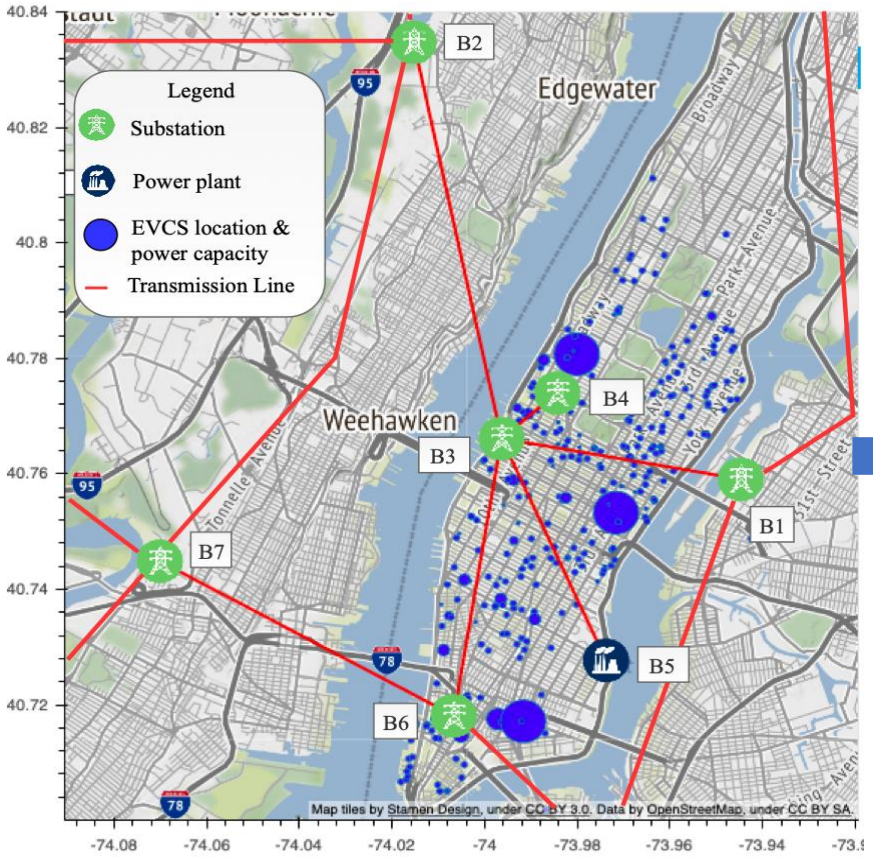


Fig: Power grid topology in Manhattan

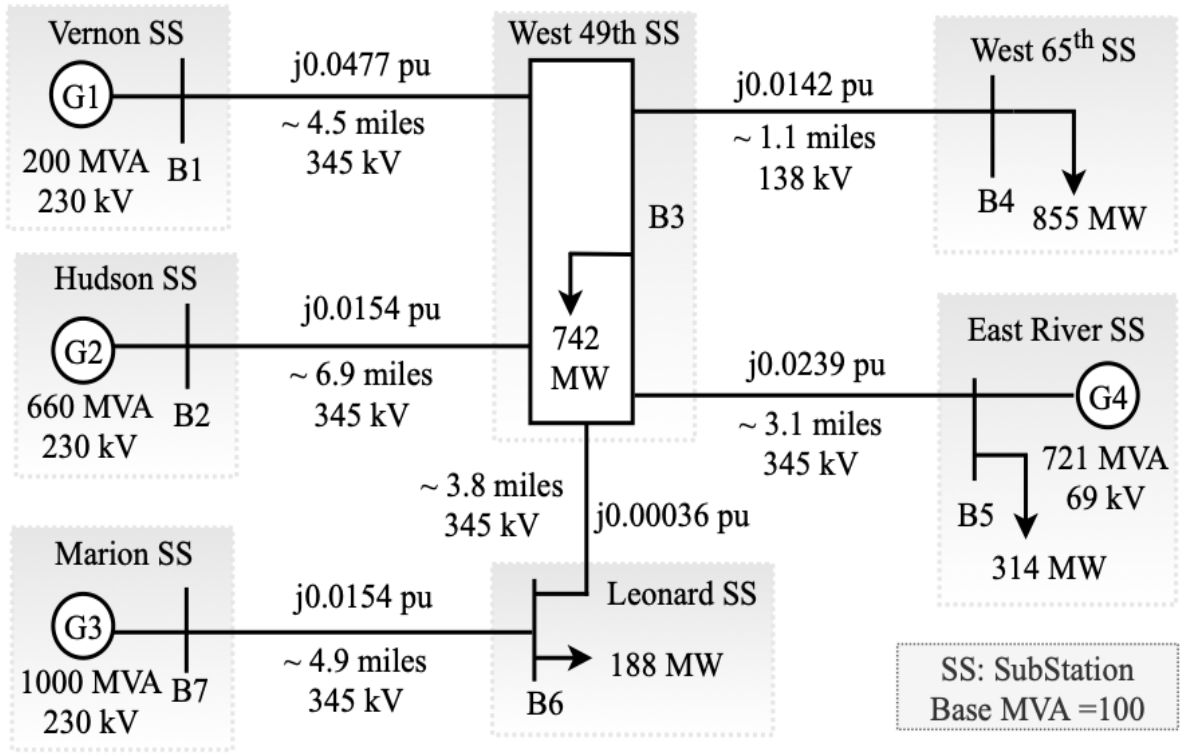


Fig: 7 node high-voltage power grid: 4 gen and 4 load nodes.

Power Grid Model

- DC power flow equations:

$$P_i^G = \sum_{k \in \mathcal{B}} Y_{ik} \Delta\delta_i, \quad \forall i \in \mathcal{G},$$

$$P_j^L = -\sum_{k \in \mathcal{B}} Y_{jk} \Delta\theta_j, \quad \forall j \in \mathcal{L}$$

$$\Delta\delta_i = \begin{cases} \delta_i - \delta_k, & \forall i \in \mathcal{G},\ \forall k \in \mathcal{G}, \\ \delta_i - \theta_k, & \forall i \in \mathcal{G},\ \forall k \in \mathcal{L}, \end{cases}$$

$$\Delta\theta_j = \begin{cases} \theta_j - \delta_k, & \forall j \in \mathcal{L},\ \forall k \in \mathcal{G}, \\ \theta_j - \theta_k, & \forall j \in \mathcal{L},\ \forall k \in \mathcal{L}. \end{cases}$$

- Generator's swing equations:

$$M_i \dot{\omega}_i = P_i^M - P_i^G - D_i^G \omega_i,$$

$$\dot{\delta}_i = \omega_i,$$

- Turbine-governor controller:

$$P_i^M = -\left(K_i^P \omega_i + K_i^I \int_0^T \omega_i \right),$$

- Nodal Demand breakdown:

$$P_j^L = \overline{P}_j^L - D_j^L \theta_j + \Delta P_j^L, \quad \forall j \in \mathcal{L}$$

Power Grid Model

- Grid dynamic equations:

$$M_i\dot{\omega}_i = -\left(K_i^P - D_i^G\right)\omega_i - K^I\delta_i - \sum_{k\in B} Y_{ik}\Delta\delta_i, \forall i \in \mathcal{G},$$

$$0 = \overline{P}_j^L - D_j^L\theta_j + \Delta P_j^L + \sum_{k\in B} Y_{jk}\Delta\theta_i, \forall j \in \mathcal{L},$$

$$\dot{\delta}_i = \omega_i, \ \forall i \in \mathcal{G}.$$

- Dimensions:

$E \in \mathbb{R}^{(2G+L)\times(2G+L)}, \hat{A} \in \mathbb{R}^{(2G+L)\times(2G+L)}, \hat{B} \in \mathbb{R}^{(2G+L)\times 1}$

$x \in \mathbb{R}^{(2G+L)\times 1}, \delta \in \mathbb{R}^{G\times 1}, \omega \in \mathbb{R}^{G\times 1}, \theta \in \mathbb{R}^{L\times 1}, u \in \mathbb{R}$

$Y_{GG} \in \mathbb{R}^{G\times G}$, $Y_{GL} \in \mathbb{R}^{G\times L}$, $Y_{LG} \in \mathbb{R}^{L\times G}$, $Y_{LL} \in \mathbb{R}^{L\times L}$

$D^G \in \mathbb{R}^{G\times G}$, $K^P \in \mathbb{R}^{G\times G}$, $K^I \in \mathbb{R}^{G\times G}$, $D^L \in \mathbb{R}^{L\times L}$, $I^{G\times G}$

$\hat{I} \in \mathbb{R}^{L\times 1}$ Single–node attack

- LTI State Space equations:

$$E\dot{x} = \hat{A}x + \hat{B}u \qquad \dot{x} = Ax + Bu$$

- Inputs and states:

$$x = [\delta, \ \omega, \ \theta]^T$$

$$u_j = \Delta P_j^L + \overline{P}_j^L$$

$$A = \overbrace{\begin{bmatrix} I & 0 & 0 \\ 0 & -M & 0 \\ 0 & 0 & D^L \end{bmatrix}^{-1}}^{E^{-1}} \overbrace{\begin{bmatrix} 0 & I & 0 \\ K^I + Y_{GG} & K^P + D^G & Y_{GL} \\ Y_{LG} & 0 & Y_{LL} \end{bmatrix}}^{\hat{A}}$$

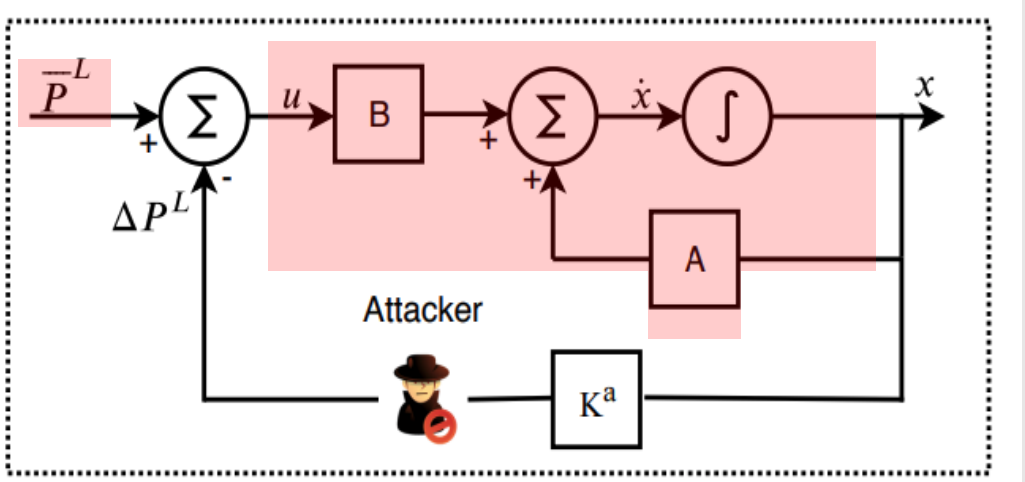
$$B = \underbrace{\begin{bmatrix} I & 0 & 0 \\ 0 & -M & 0 \\ 0 & 0 & D^L \end{bmatrix}^{-1}}_{E^{-1}} \underbrace{\begin{bmatrix} 0 \\ 0 \\ \hat{I} \end{bmatrix}}_{\hat{B}}$$

Data-driven Cyberattack Model

$\dot{x} = Ax + Bu$

Unattacked Grid Model

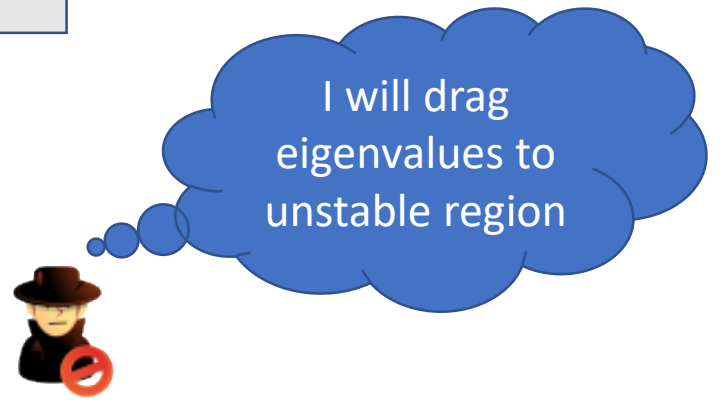
$$\dot{x} = Ax + B(\overline{P}^L - K^a x) = (A - BK^a)x + B\overline{P}^L$$



Well-known parameters

Fig: Data driven state-feedback based attack model

- Data-driven model
- Power grid instability analyzed using *eigenvalues of the system*
- Optimization of K^a ?
- $K^a x = \Delta P^L$; $0 \leq K^a x \leq \Delta P^{max}$

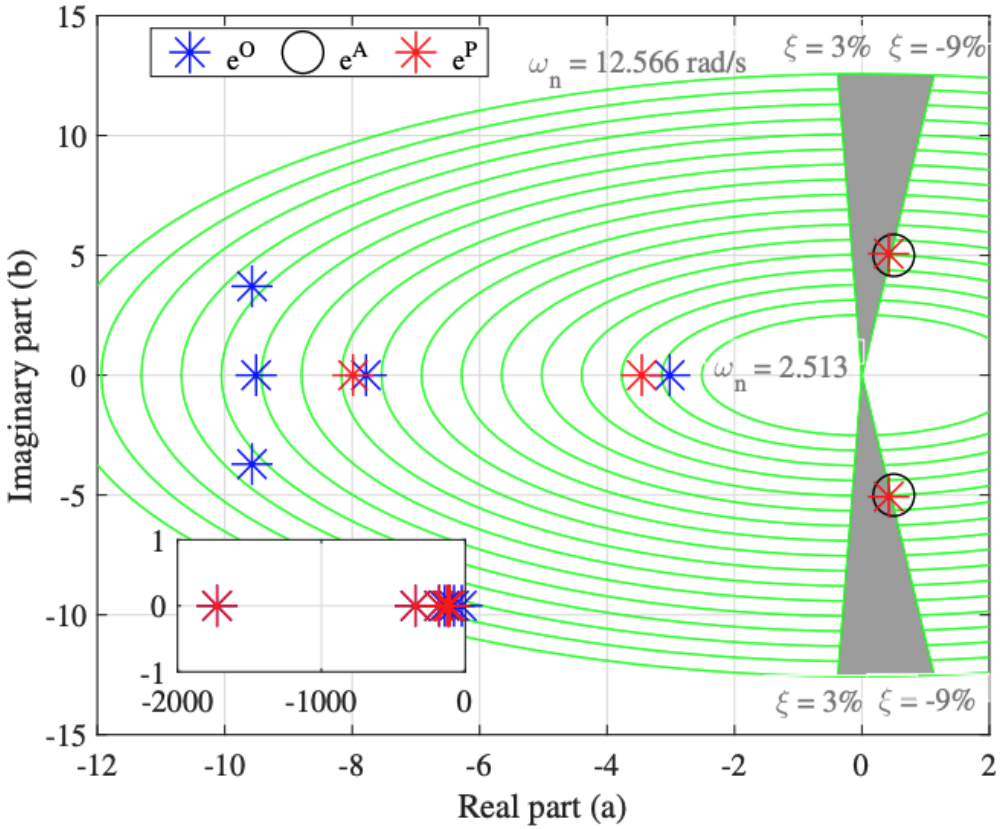


Case Study: EV Destabilizing the Grid

- Destabilize grid via eigenvalue relocation
- 4 Gen nodes, 4 load nodes
- 4 δ, 4 ω, 4θ, 12 eigenvalues
- Not fully controllable
- Attacker's target ; $e^a = a + jb = 0.5 \pm j5$
- 355 MW could succeed the attack


1K x

(with 350 kW chargers)



Relocation of the eigenvalues under attack on node B4, where e^o denotes original (pre-attack) eigenvalues and e^a denotes eigenvalue locations targeted by the attacker. The post-attack eigenvalues are denoted as e^p. Green lines represent ξ and ωn and the gray shaded area represents S^a.

Note: $a = -\xi\omega_n, \quad b = \omega_n\sqrt{1-\xi^2}$

Case Study: EV Destabilizing the Grid

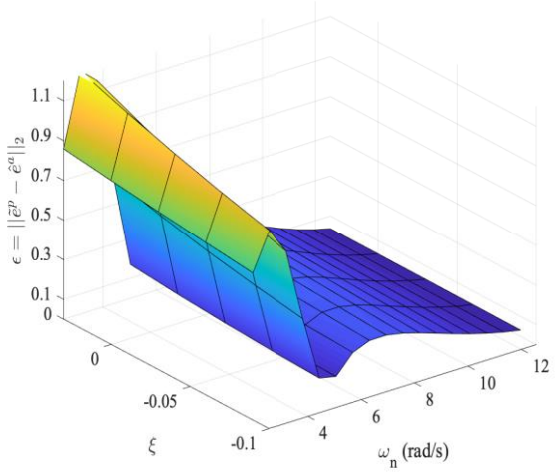
- The North American Electric Reliability (NERC) defines a region of vulnerability:

$$S^a \in \mathbb{C} : \{\xi \leq 3\%, \quad 2.5 \leq \omega_n \geq 12.6\ rad/s\}.$$

- S^a discretized: $\xi = 0.3\%,\ \omega_n = 0.1\ rad/s$

$$\hat{e}^a : \{\hat{\xi}, \hat{\omega}_n\} \in \hat{S}^a$$

720x  (with 350 kW chargers)



Maximum relocation error $\varepsilon = \left|\left|\tilde{e}^p - \tilde{e}^a\right|\right|_2$ for different $\{\hat{\xi}, \hat{\omega}_n\} \in \hat{S}^a$ chosen by the attacker, where. $\tilde{e}^p$ are the two nearest eigenvalues to $\hat{e}^a$.

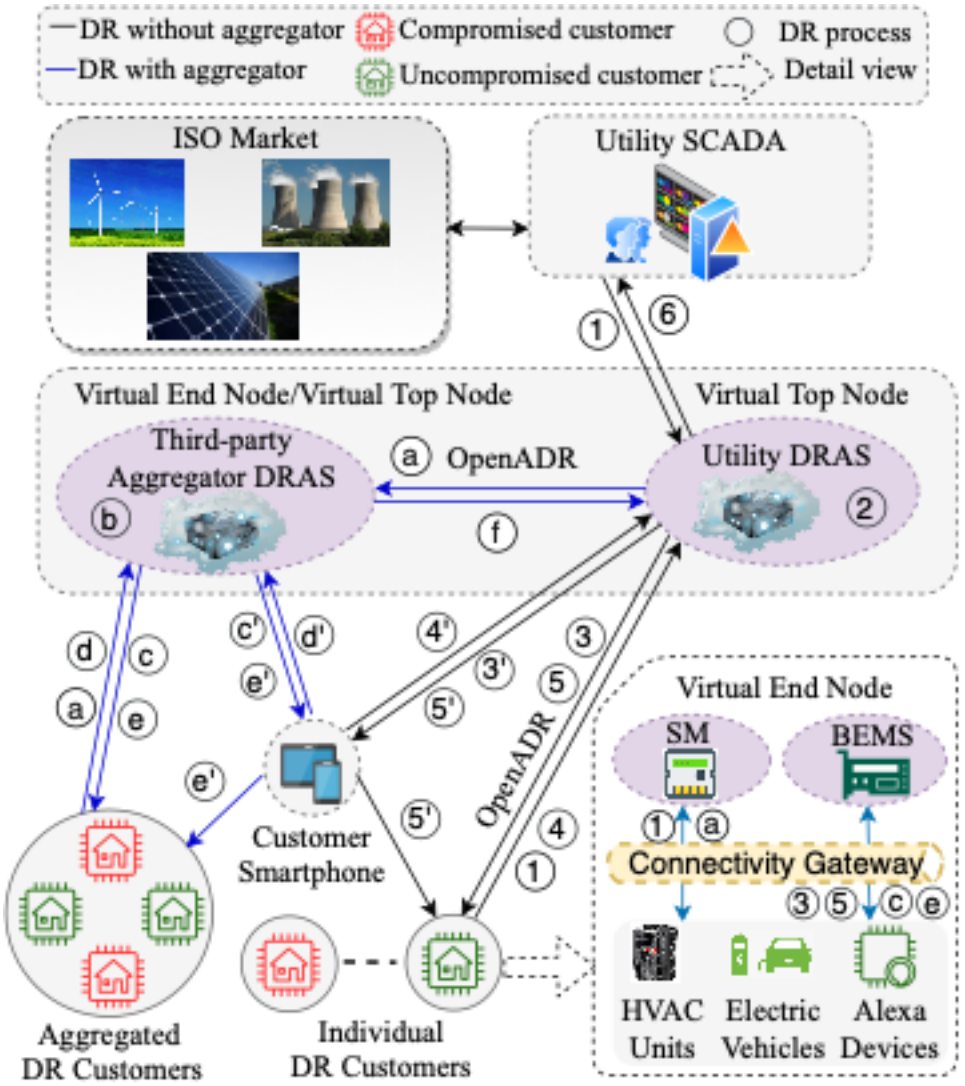
ΔP^L (MW) associated with $\varepsilon \leq 0.1$

$\omega_n(rad/s)$	ξ				
	-0.09	-0.06	-0.03	0	0.03
5.7	352.1	347.2	342.2	337.1	332
10.7	303.5	295.6	N/A*	N/A*	N/A*
11.3	297.1	289.4	281.8	274.1	266.6
11.9	290.6	283.2	275.8	268.5	261.2
12.6	283.9	276.7	269.6	262.6	255.7

* Value corresponds to $\varepsilon > 0.1$ and labeled not available (N/A)

Demand Response Model

- DR without aggregators (1 – 6)
- DR with aggregators (a –f)
- Data from Smart Meters and ISO market
- AI in DRAS
- Vulnerable home IoT ➔ Smart Meters
- No system wide communication standard
- Smartphones in middle of DR



S. Acharya, Y. Dvorkin, and R. Karri, "Causative Cyberattacks on Online Learning-based Automated Demand Response Systems", IEEE Transactions on Smart Grid, 2021

Demand Response Attack Model

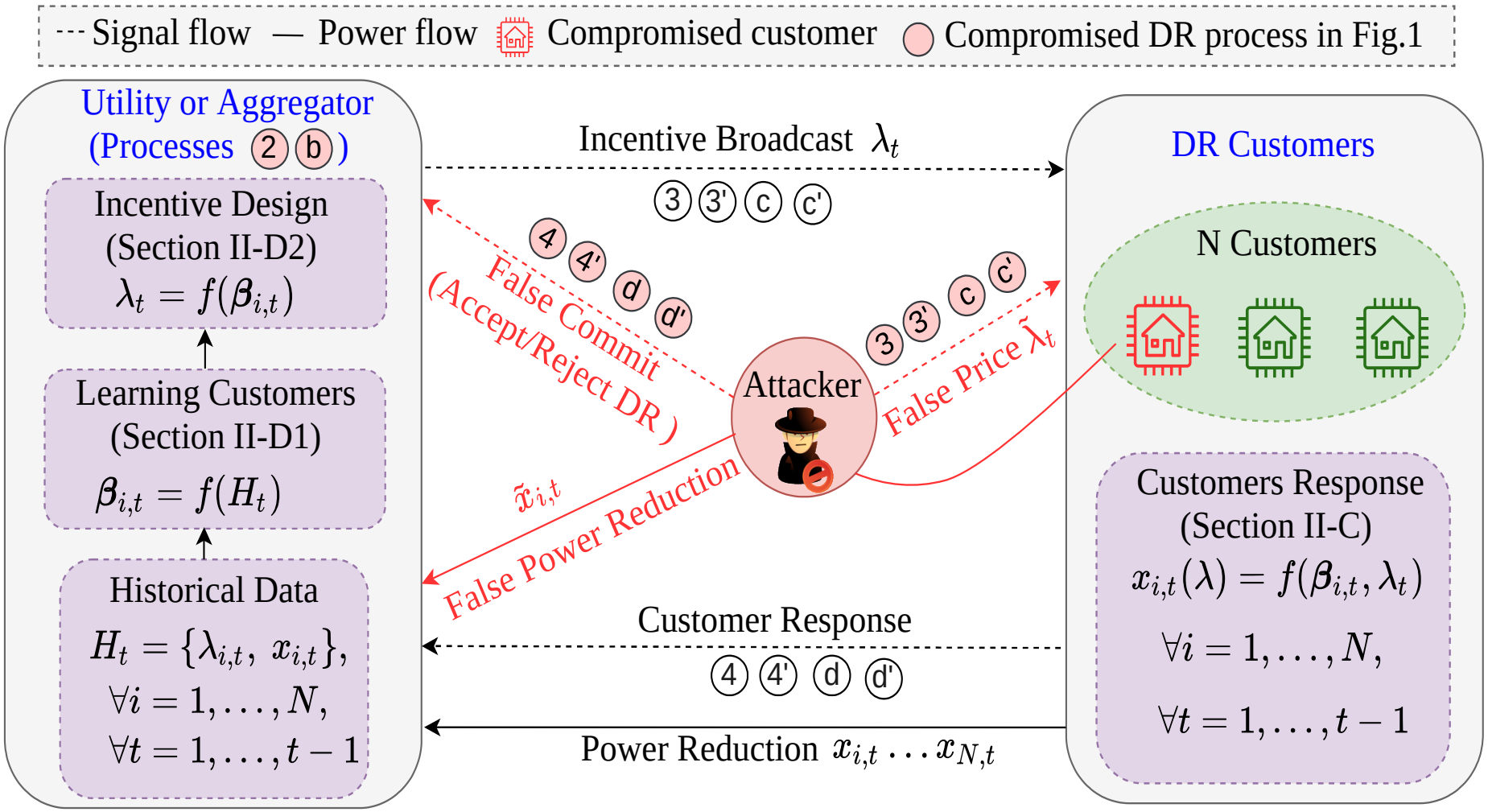


Fig: Attack mechanism

Case Study: NYU Microgrid

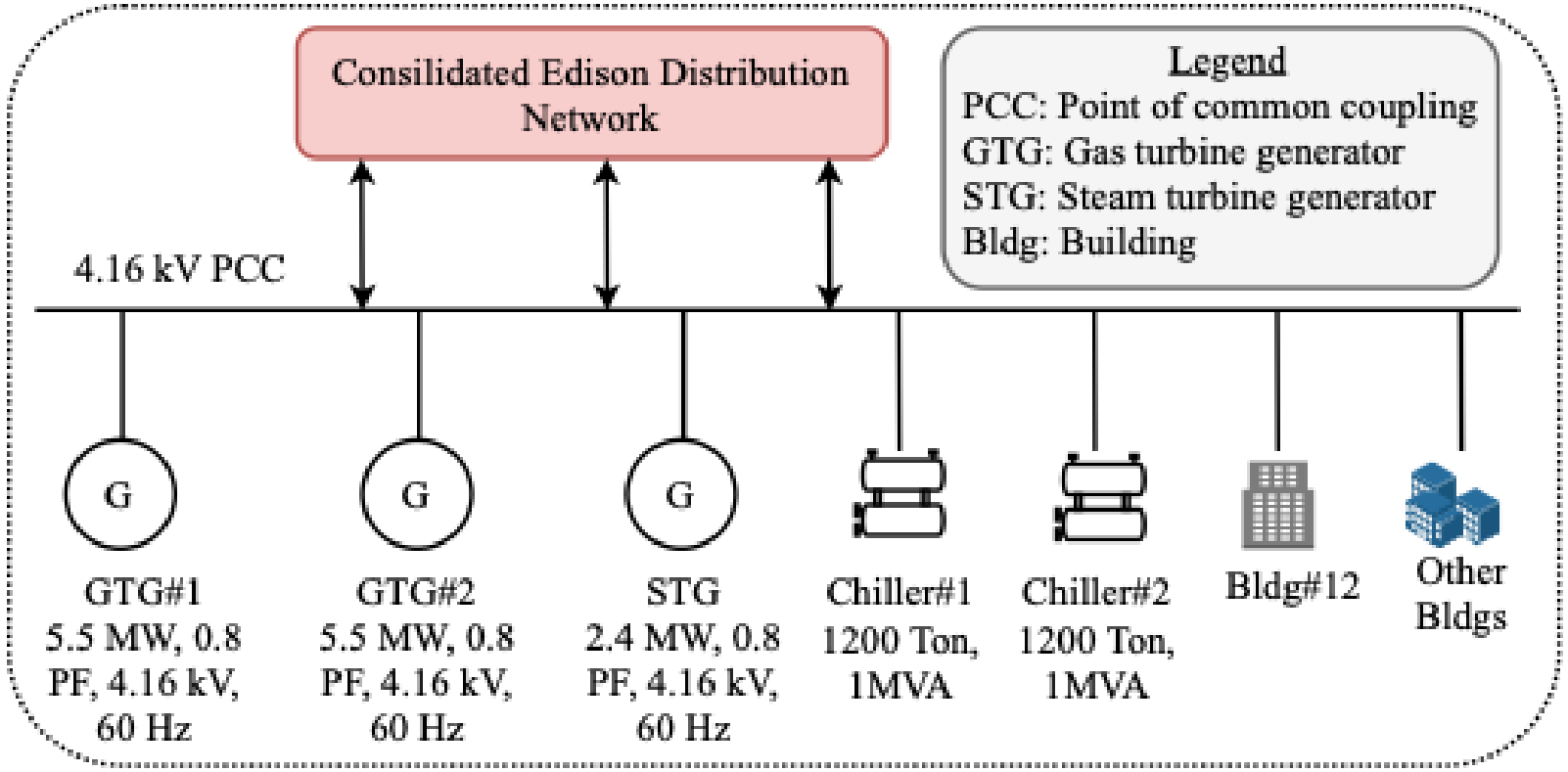


Fig: Schematic of NYU microgrid.

Case Study: Demotivating Grid from DR

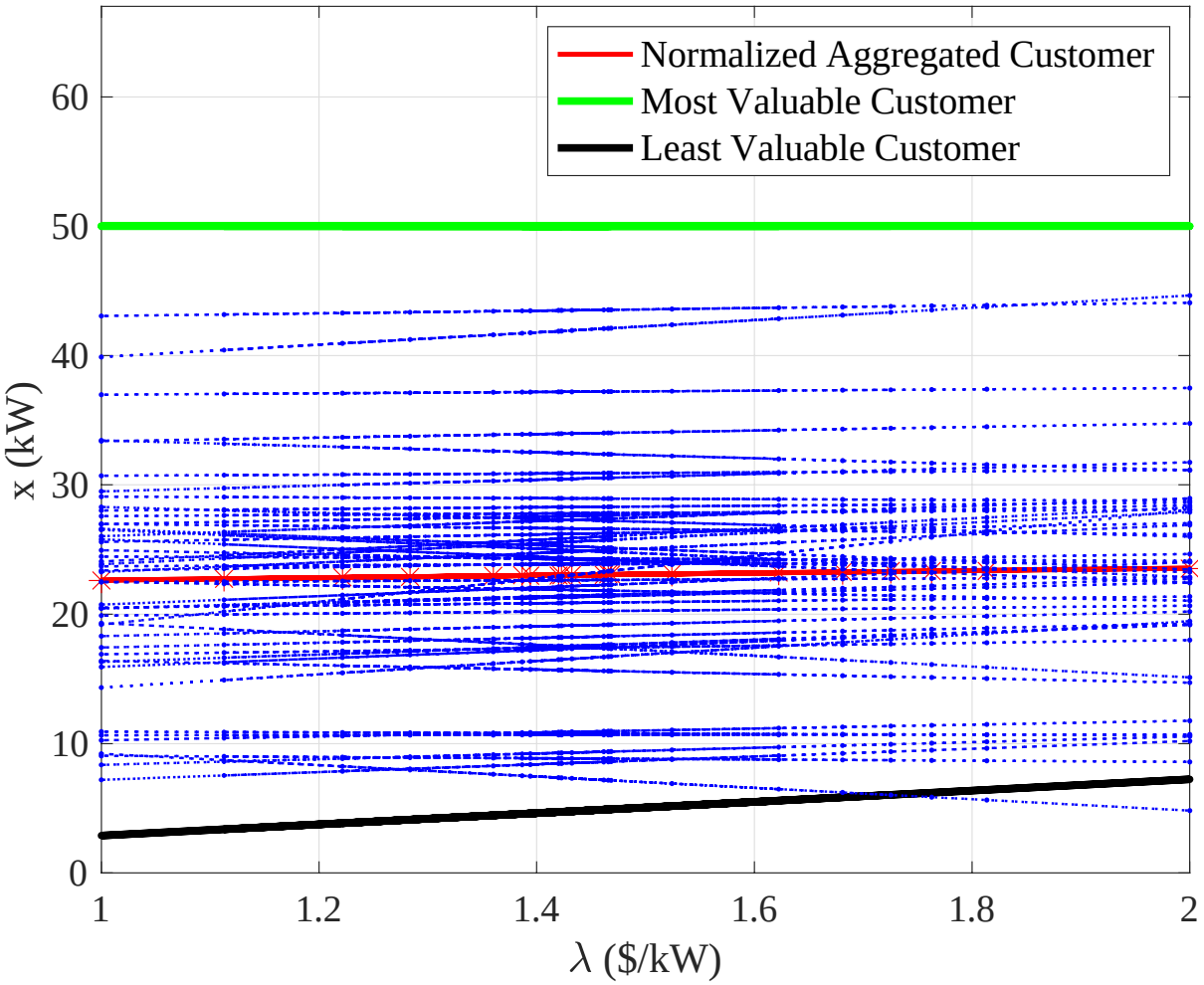


Fig: Attack valued DR customers

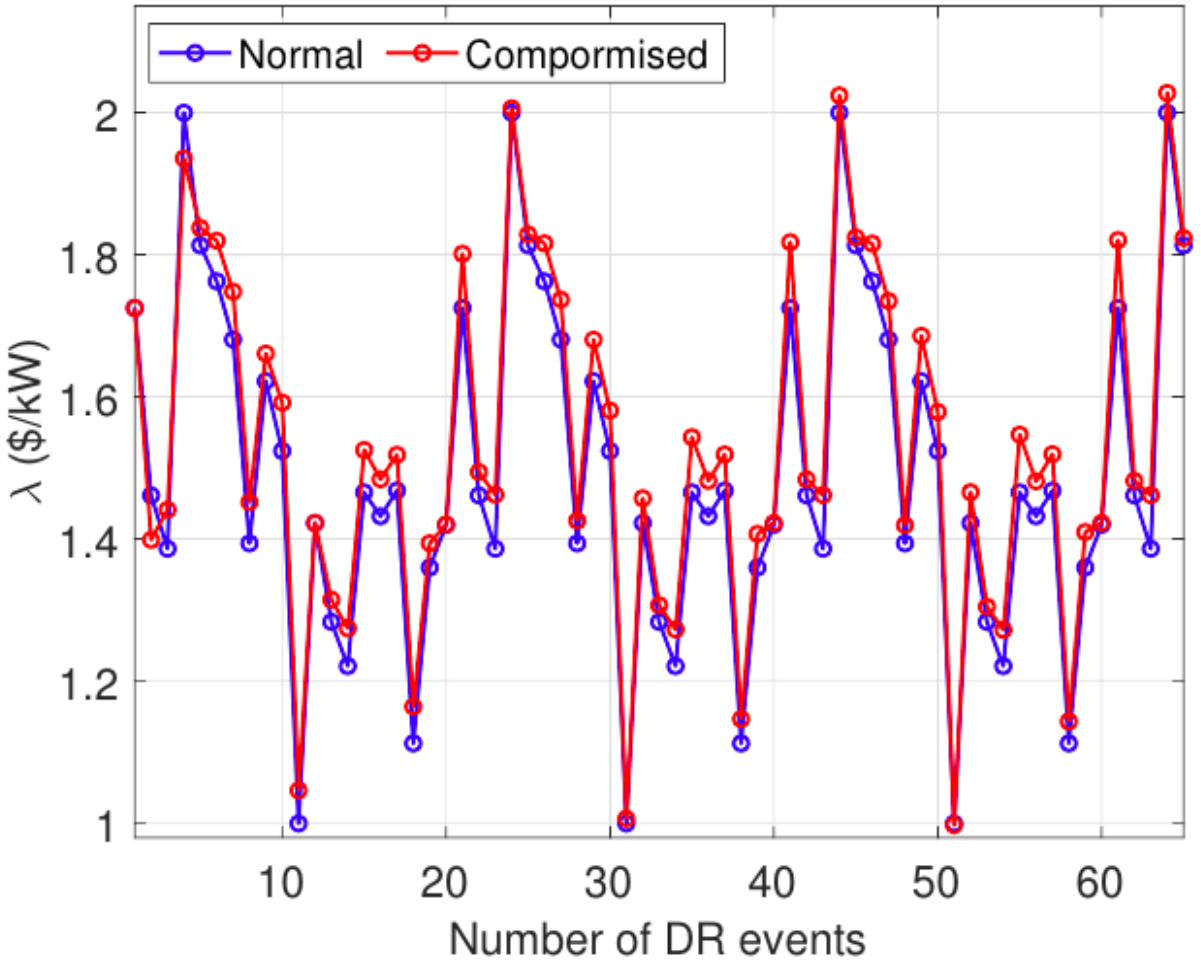


Fig: Stealthy increase of DR incentive by manipulating as less as 30 % DR customers.

Case Study: Technical challenges in Grid

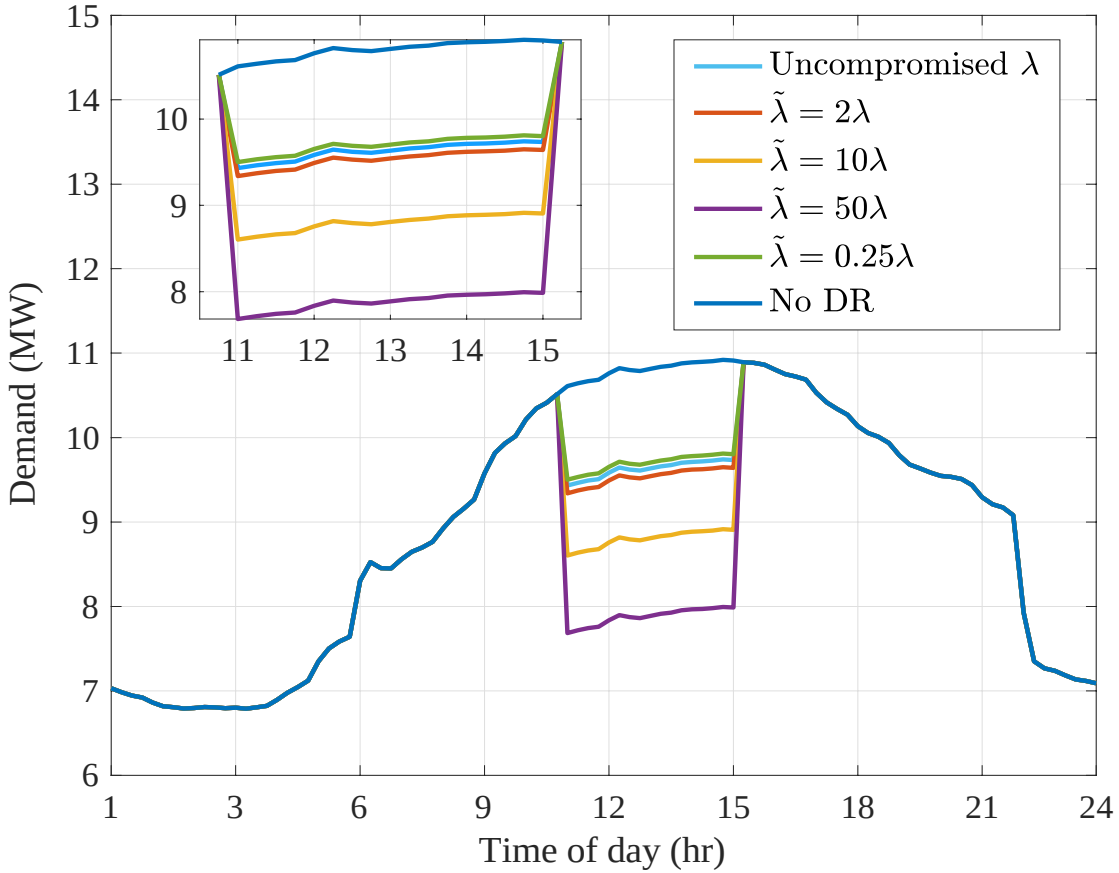


Fig: Changes in NYU microgrid demand caused by the attacks.

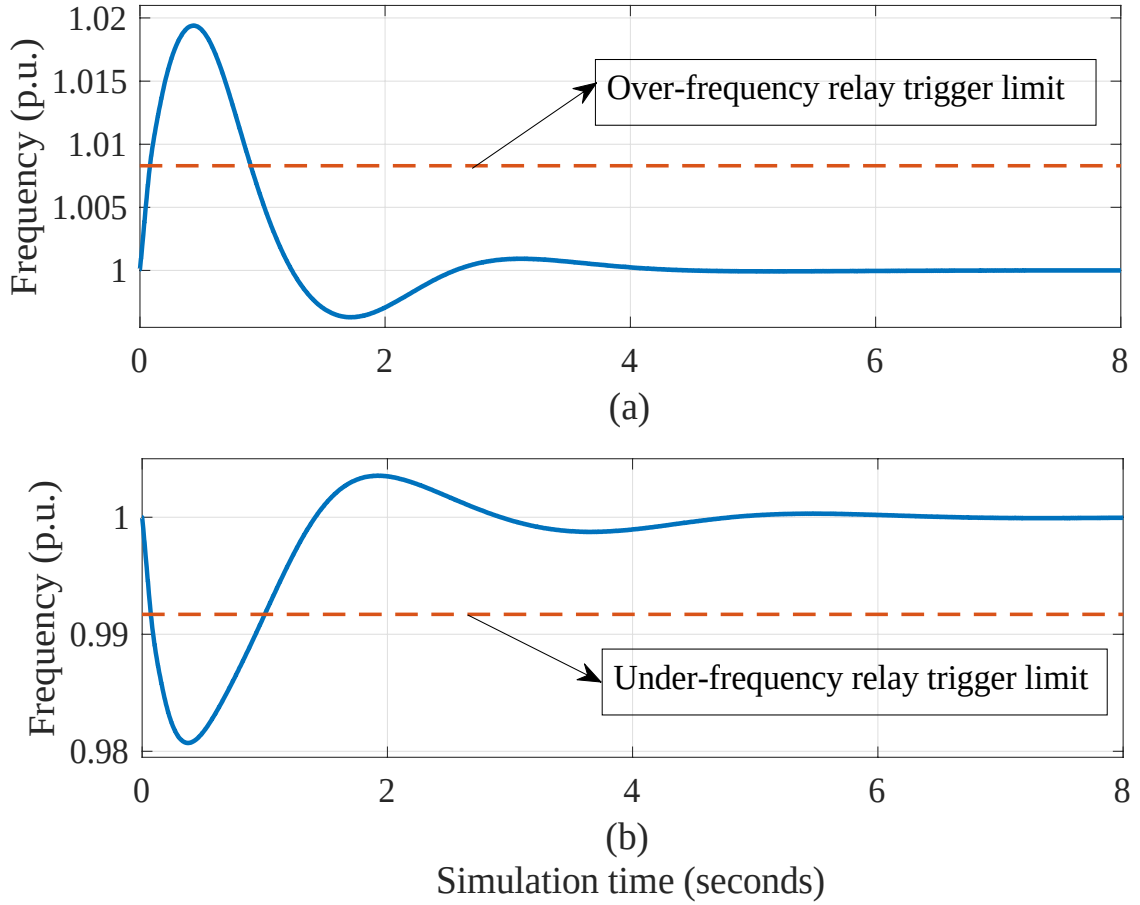


Fig: Microgrid frequency in response to the attacks.

Cyber Insurance as a defense?

- Defense is not a 100% guarantee.
- Many can’t even afford the shield or are unaware.
- Cyber insurance: Can’t avoid attack but saves from business loss.

Cyber Insurance Market

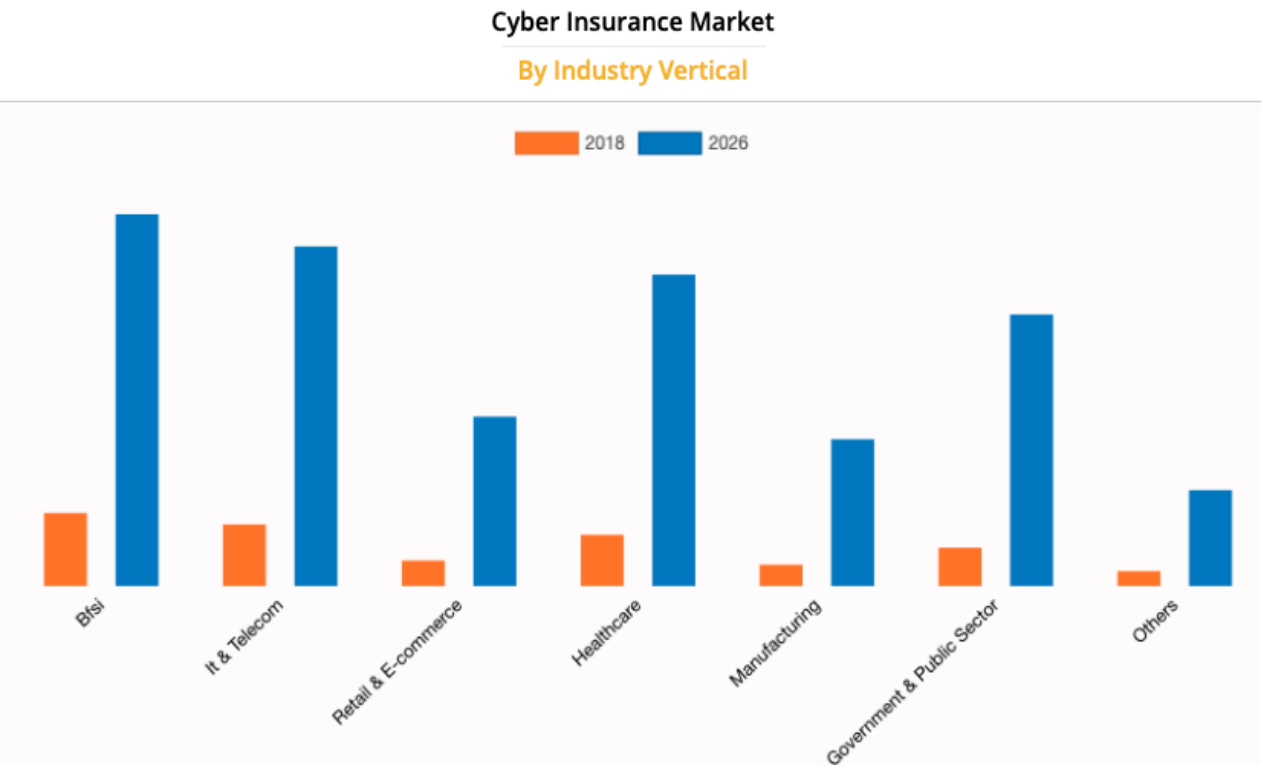


Fig: Cyber Insurance Market Trend.

- Energy sector share in insurance market?

US P/C Industry – Top 20 Cyber Insurers, 2018-2019

($ millions)

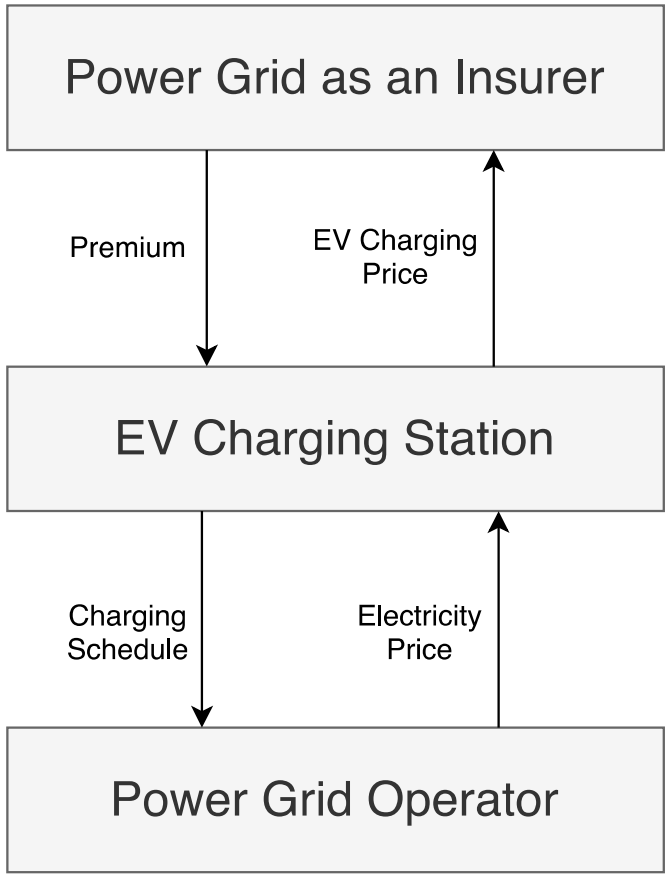
Rank 2018	Rank 2019	Company Name	2019 DPW	2018-2019 DPW Change (%)	Market Share (%)	% of Cybersecurity DPW Standalone	% of Cybersecurity DPW Packaged
1	1	Chubb INA Group	356.9	9.5	15.9	0.4	99.6
2	2	XL Reinsurance America Group (AXA XL)	229.7	-10.2	10.2	100.0	0.0
3	3	American International Group	225.8	-2.9	10.0	99.5	0.5
4	4	Travelers Group	178.5	22.1	7.9	80.7	19.3
5	5	Beazley USA Insurance Group	150.9	36.0	6.7	93.8	6.2
7	6	AXIS US Operations	97.3	28.0	4.3	51.0	49.0
6	7	CNA Insurance Companies	94.7	13.6	4.2	16.9	83.1
8	8	BCS Financial Group	76.1	9.4	3.4	58.7	41.3
9	9	Liberty Mutual Insurance Companies	68.4	2.8	3.0	43.4	56.6
14	10	Fairfax Financial (USA) Group	65.1	70.4	2.9	99.8	0.2
12	11	Hartford Insurance Group	57.5	28.7	2.6	13.5	86.5
10	12	Tokio Marine US PC Group	52.6	10.7	2.3	66.9	33.1
13	13	Sompo Holdings US Group	49.7	22.3	2.2	47.1	52.9
11	14	Zurich Insurance US PC Group	49.2	6.8	2.2	88.4	11.6
15	15	Berkshire Hathaway Insurance Group	31.2	8.8	1.4	38.8	61.2
19	16	W. R. Berkley Insurance Group	23.9	23.1	1.1	72.8	27.2
20	17	The Cincinnati Insurance Companies	21.7	29.0	1.0	0.0	100.0
18	18	Aspen US Insurance Group	19.6	-7.8	0.9	99.0	1.0
16	19	Markel Corporation Group	19.5	-13.2	0.9	57.0	43.0
23	20	Alleghany Corporation Group	19.3	45.4	0.9	66.8	33.2
		Top 5*	**1,141.8**	**6.6**	**50.7**	**66.0**	**34.0**
		Top 10*	**1,543.4**	**9.1**	**68.6**	**61.4**	**38.6**
		Top 20*	**1,887.5**	**10.1**	**83.9**	**58.2**	**41.8**
		Total P/C Industry	**2,250.9**	**11.9**	**100.0**	**54.6**	**45.4**

Ranked by 2019 total standalone and packaged cybersecurity direct premiums written.

Source: AM Best data and research

Fig: Cyber Insurance Market Size.

Power Grid as an Insurer



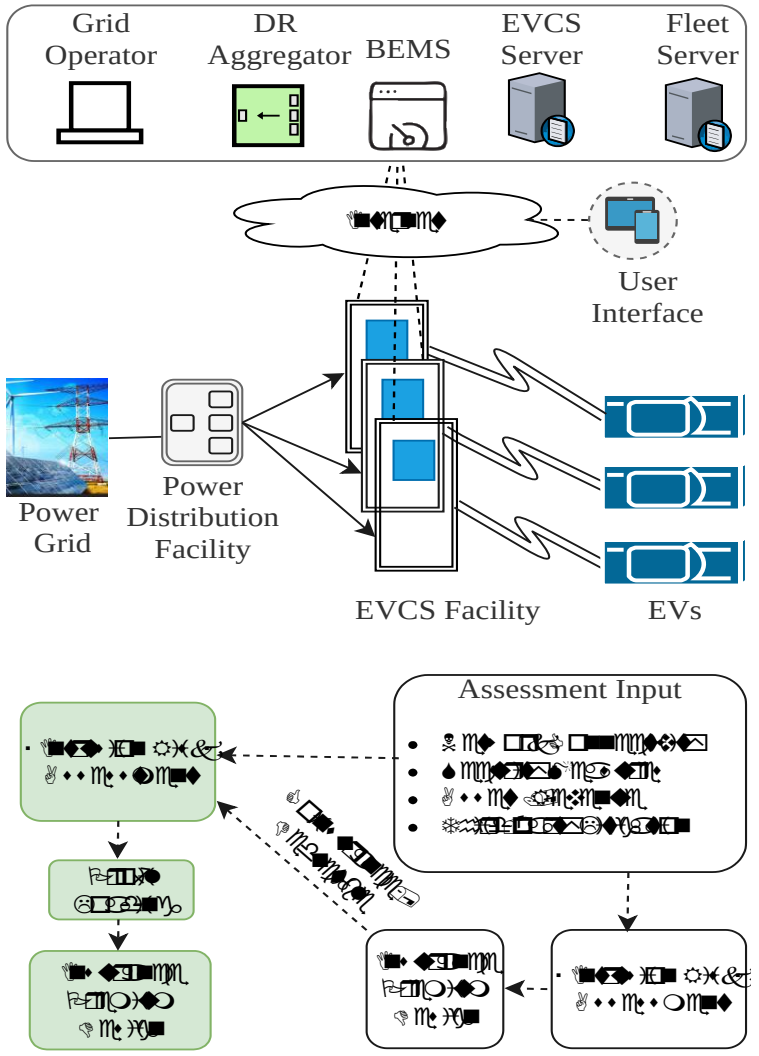


Fig: A game-theoretic model of cyber insurance premium design.

Conclusion

- Demand-Side Cyberattacks base on customer cyber hygiene.
- Grids leaving high-wattage devices unmonitored.
- Public data incurring security and privacy issue.
- Cyber consensus among power grid and demand-side service providers to develop business standards and cyber responsibilities.
- Cyber insurance could be a solution to foster small green business.

Thank you !