Balancing Smart Grid's Performance Enhancement and Resilience to Cyber Threat

Rezoan A. Shuvro, Pankaz Das, and Majeed M. Hayat

Department of Electrical and Computer Engineering,

Marquette University, Milwaukee, WI, USA

Outline

Motivation for this work

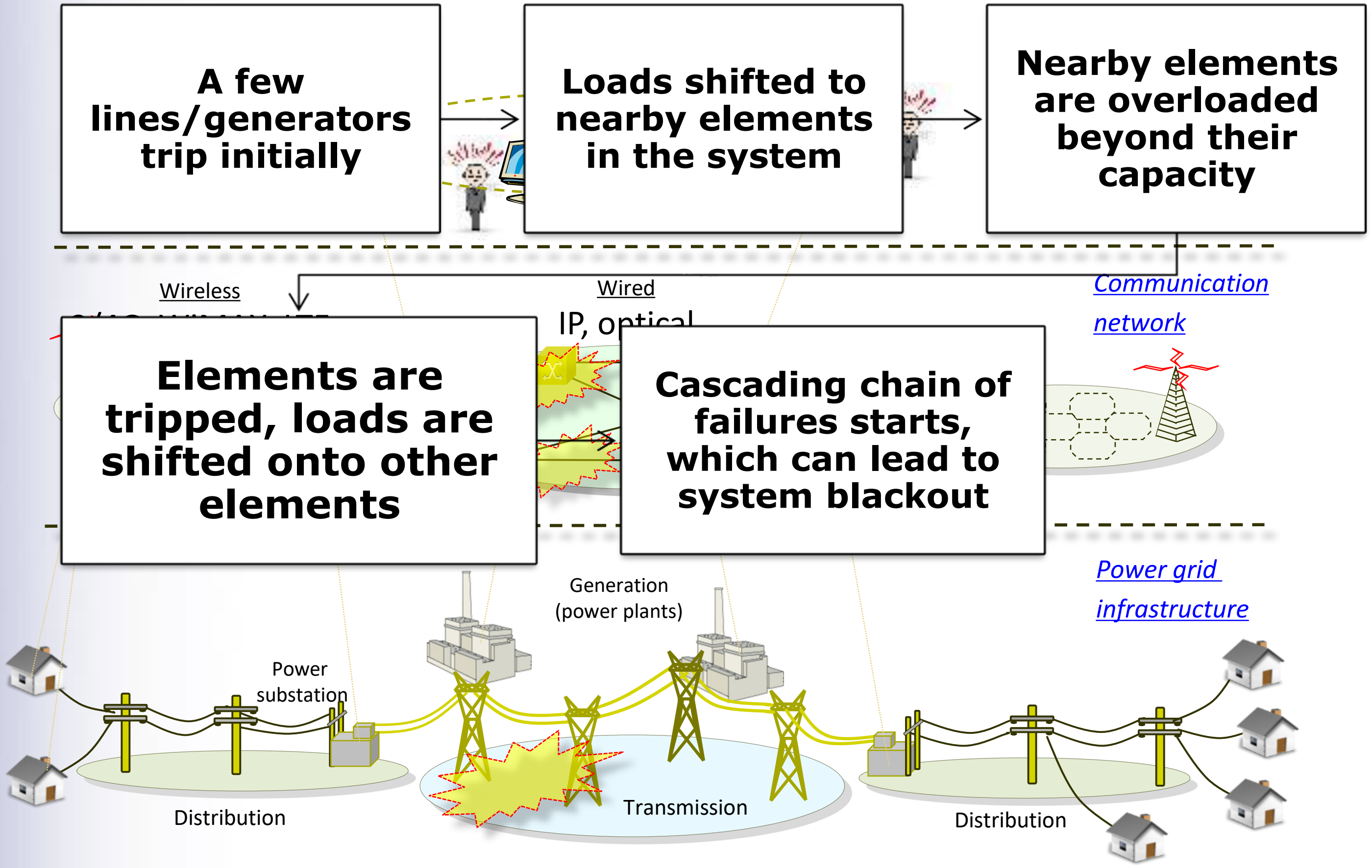
Contributions of this work

Methodology

Results

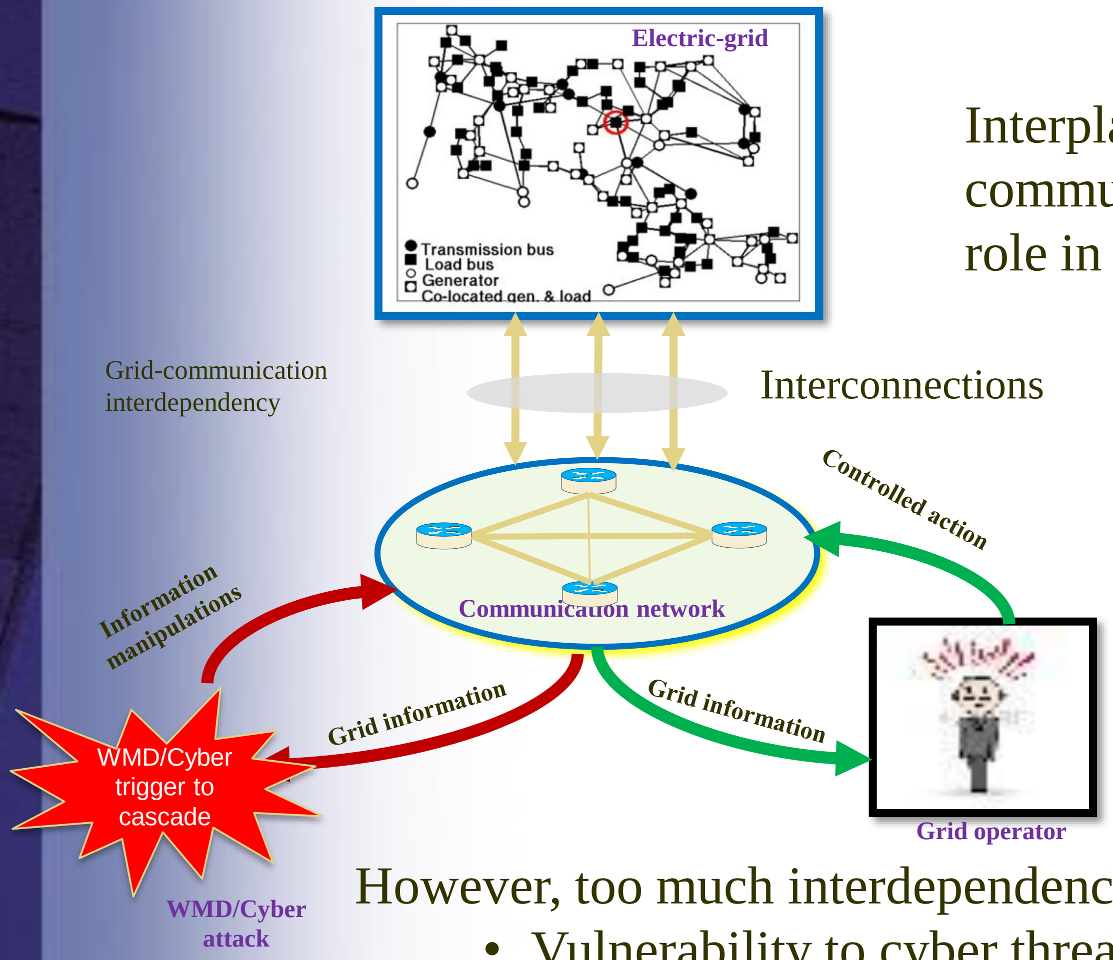
Conclusions and Extensions

Interdependencies in smart grids



How the interdependencies among these layers affect the reliability and resiliency of the smart grid?

Benefit and curse of information



Interplay between electric grid and communication/control networks plays pivotal role in the reliability of smart grids.

Increased interdependency gives more information, and hence reliability through informed control.

However, too much interdependence can lead to

- Vulnerability to cyber threat.
- Higher infrastructure cost.
- Decreased robustness due to strong dependence on information.

Fundamental question: balance the tradeoff between grid's performance enhancement and robustness.

Background: our works

- Started working on modeling cascading failures (2011)
- Markov chain based analytic cascading failure model (2014)
- Interdependent Markov chain cascading failure model (2016)
- Capturing the role of operator error in interdependent Markov chain model (2018)
- Balancing trade-off between grids performance and resilience to cyber threat (2019)
- Ongoing work: Markov decision process for cascade mitigation (2020)

Contributions of this paper

- Developing a comprehensive 3-layer (power grid, communication, and human response) Markov chain based analytical cascading-failure model.

- The model finds the distribution of blackout size for a given initial condition of the grid.

- The model finds the optimal level of interdependence, i.e., the trade-off between well-informed control and vulnerability to attacks, that minimizes the probability of massive cascading failures in power grids.

Reduced state space for the power-grid variables

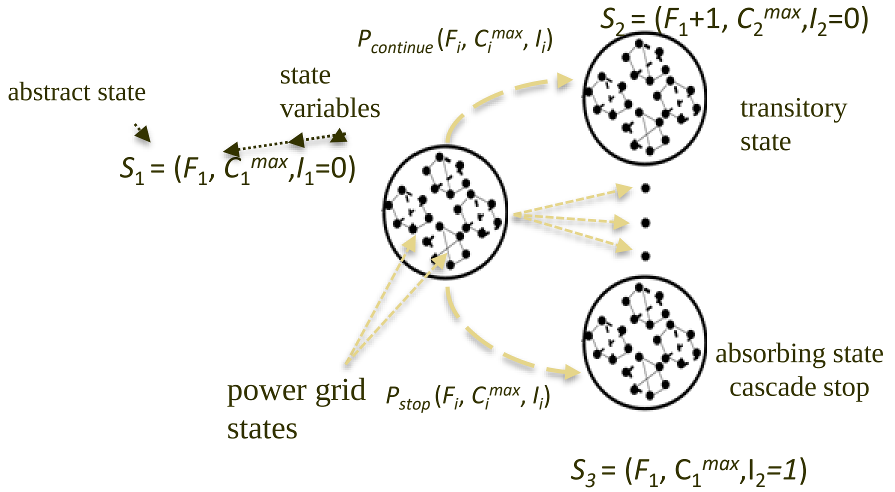
Main ideas of the *stochastic abstract-state evolution (SASE)* approach [1]:

- Simplify the state space of the complex power system (**equivalence classes**)

  Aggregate state variables: $\boldsymbol{S_i = (F_i, C_i^{\max}, I_i)}$

  F: number of failed lines
  ***C**^max*: maximum capacity of failed lines
  I: cascade-stability of the power grid

- Capturing the effects of the omitted variables through the transition probabilities for *I* and their parametric dependence on physical attributes and **operating characteristics** of the system.



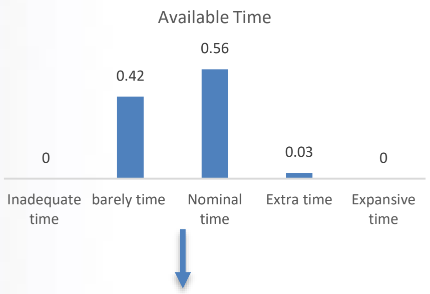
Dynamics of the reduced states is represented by a Markov chain.

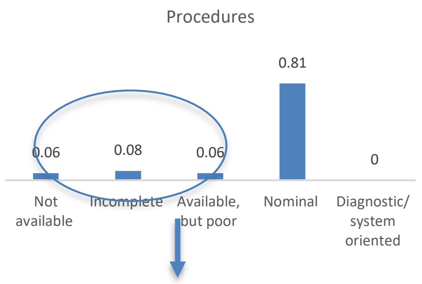
1. Rahnamay-Naeini, M., Wang, Z., Ghani, N., Mammoli, A., & Hayat, M. M. (2014). Stochastic analysis of cascading-failure dynamics in power grids. *IEEE Transactions on Power Systems*, *29*(4), 1767-1779.

Power grid and human operators' interdependency

- Idea: number and maximum capacity of failed transmission lines increases the human-error probability in decision making.
- Standardized Plant Analysis Risk-Human (SPAR-H) reliability analysis method was used to calculate human-error probability (HEP) through performance shaping factors (PSFs).
- Mapping between (F, C^{max}) and operator response level, H, is established while considering human-error probability, HEP, and the distribution of the PSFs [1].

Distribution of the PSFs were calculated empirically.





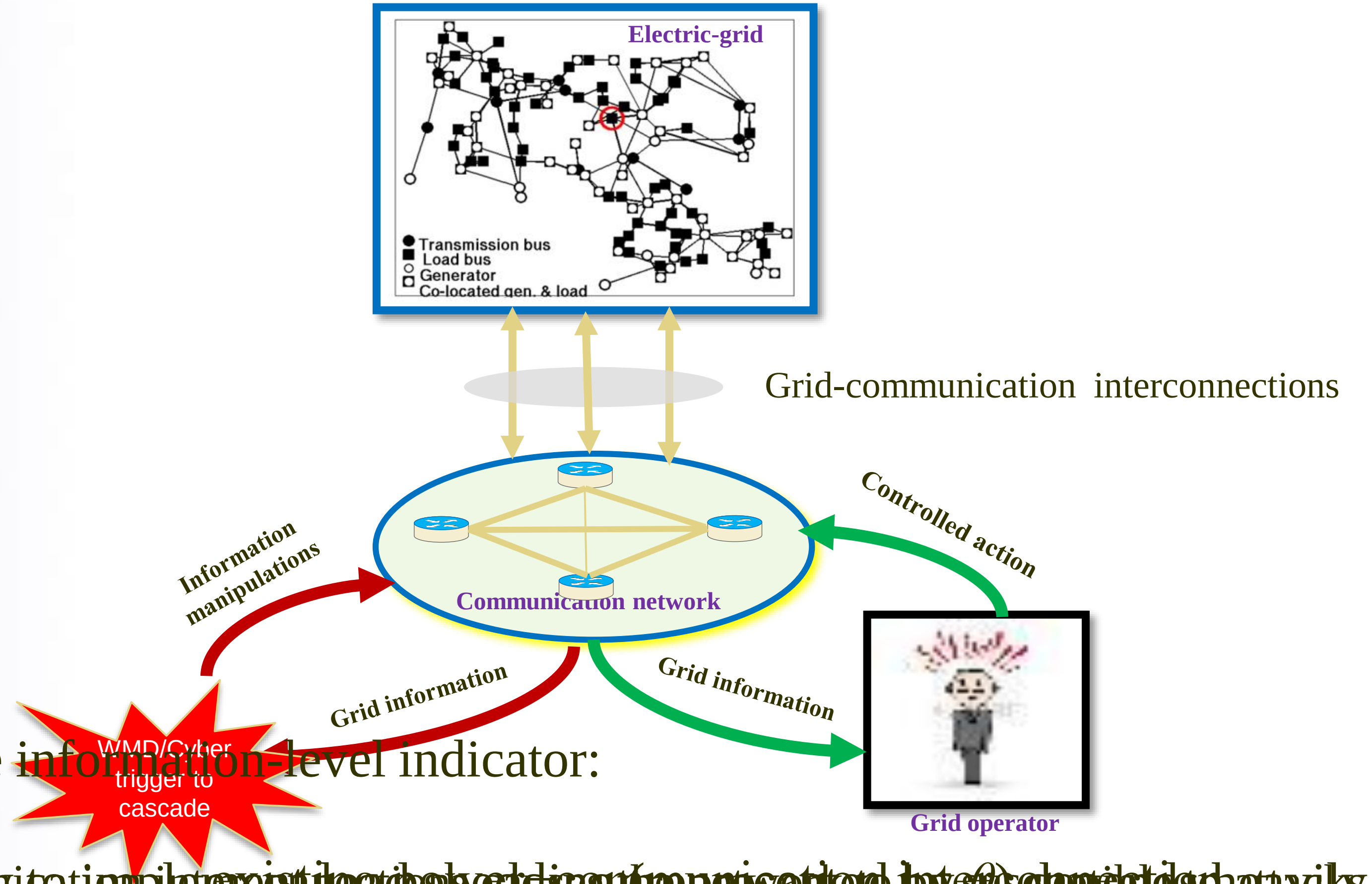
There are always time constraints

Procedures are mostly available

Operators reported they were always fit.

1. Rezoan A. Shuvro, Pankaz Das, Joana M. Abreu, and Majeed M. Hayat. "Correlating Grid-operators' Performance with Cascading Failures in Smart-Grids." ISGT-Europe, 2019.

Power grid, human operators and communication network interdependencies



- Consider the information-level indicator:

$$k = \frac{\text{number of existing power-communication interconnections}}{\text{maximum number of possible power-communication interconnections}}$$

- k changes as cascading failures evolves, and θ depends on k.
- k=1 means operators have maximum information of the grid for decision making.
- k=0 means operators have minimum information of the grid for decision making.
- ψ has an inverse relationship with k.

- The capability to implement the control actions (represented by θ) depends heavily on the availability of information from the communication network.
- Power-communication interdependency increases the probability of cyber-attacks.
- To capture this phenomenon we introduced a cyber threat parameter, ψ, which captures the vulnerability of the network.
- High power-communication interdependency increases operators' control over the grid.

Constructing the Markov chain

1. Develop a cascading-failure simulator (we used **MATPOWER**), run cascading failure simulations and observe pattern.

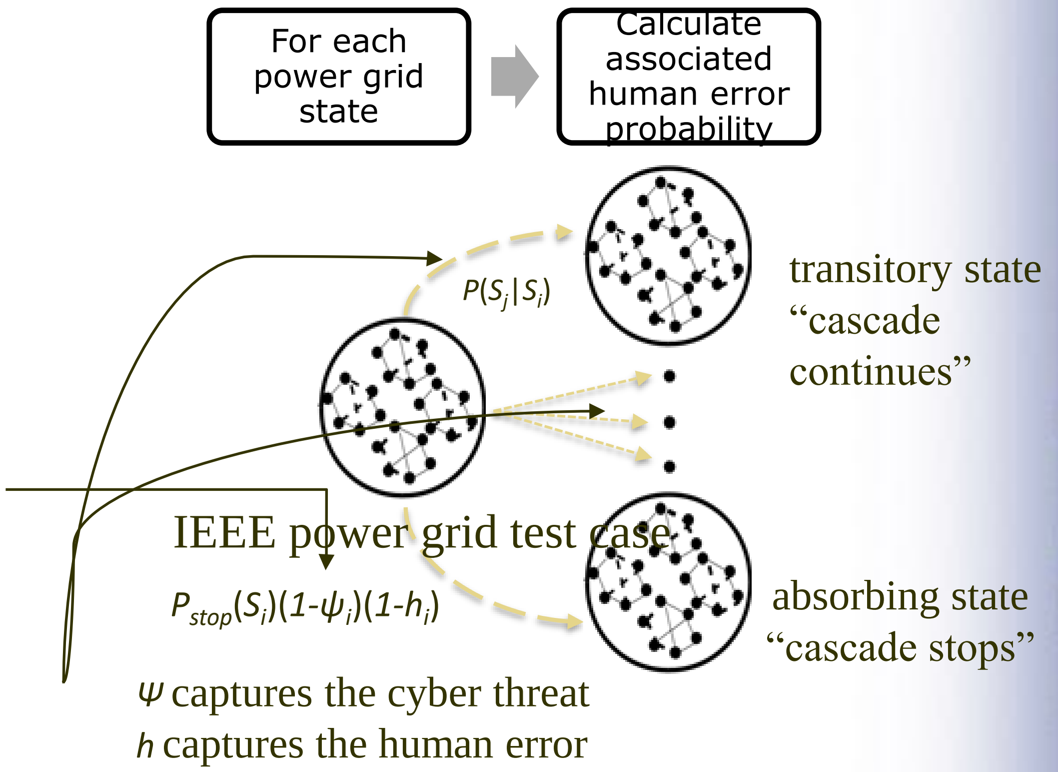
2. From the human error model and power grid failure observations, calculate the **mapping** between **power grid states** and the associated **human error level**.

3. Update the **probability of cascade stop** from the observations using equations (4-13) from the paper.

4. Dynamics of **power-communication interconnectivity** and **cyber threat** are captured using equations (1-2) from the paper.

5. Calculate the **probability of cascade-continue** at the associated capacity levels.

6. Construct the **Markov chain** transition matrix using the state-transition rules (discussed next).



State transition probabilities

- State transition probabilities capture benefits and added vulnerabilities resulting from information.

$$f(S_j|S_i) = \begin{cases} 1 & if\ F_j = F_i, C_j^{max} = C_i^{max}, I_j = I_i = 1, \\ P_{stop}(S_i)(1-\psi_i)(1-h_i) & \\ \quad if\ F_j = F_i, C_j^{max} = C_i^{max}, I_j = 1, & \\ P(S_j|S_i) & if\ F_j = F_i + 1, C_j^{max} \in \mathcal{C}, I_j = 0, \\ 0 & otherwise. \end{cases}$$

captures the dynamics of power grid.

captures the role of security threat due to exposure due to more power-communication.

captures the role of operator errors.

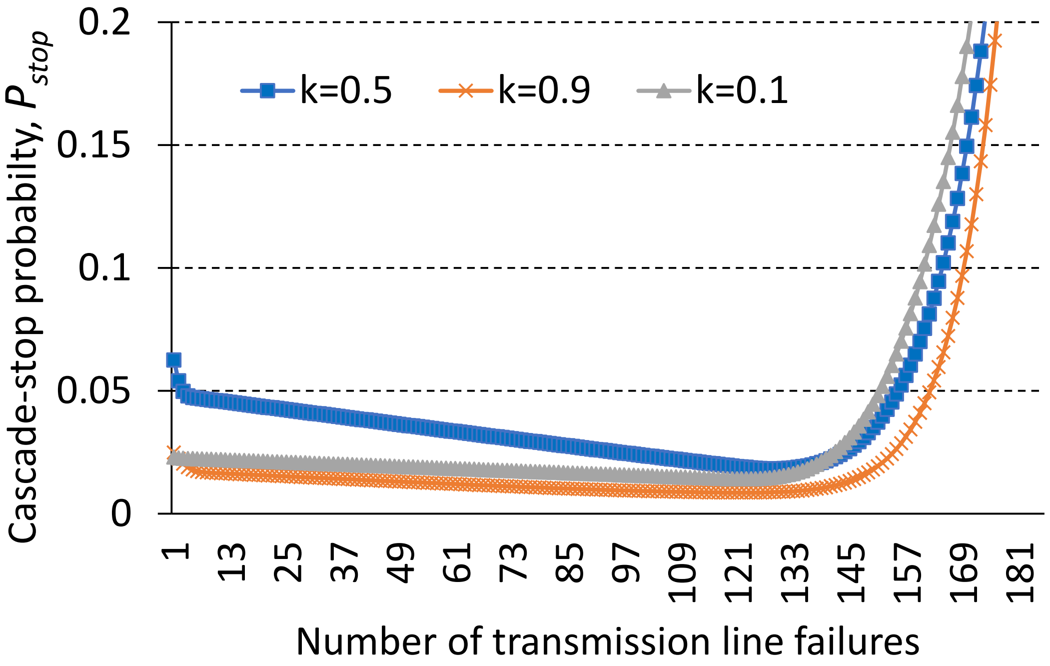
captures the transition probabilities of the Markov chain.

Results

- *Once the Markov chain is constructed using the data-driven approach, we can use it analytically for that power grid topology.*

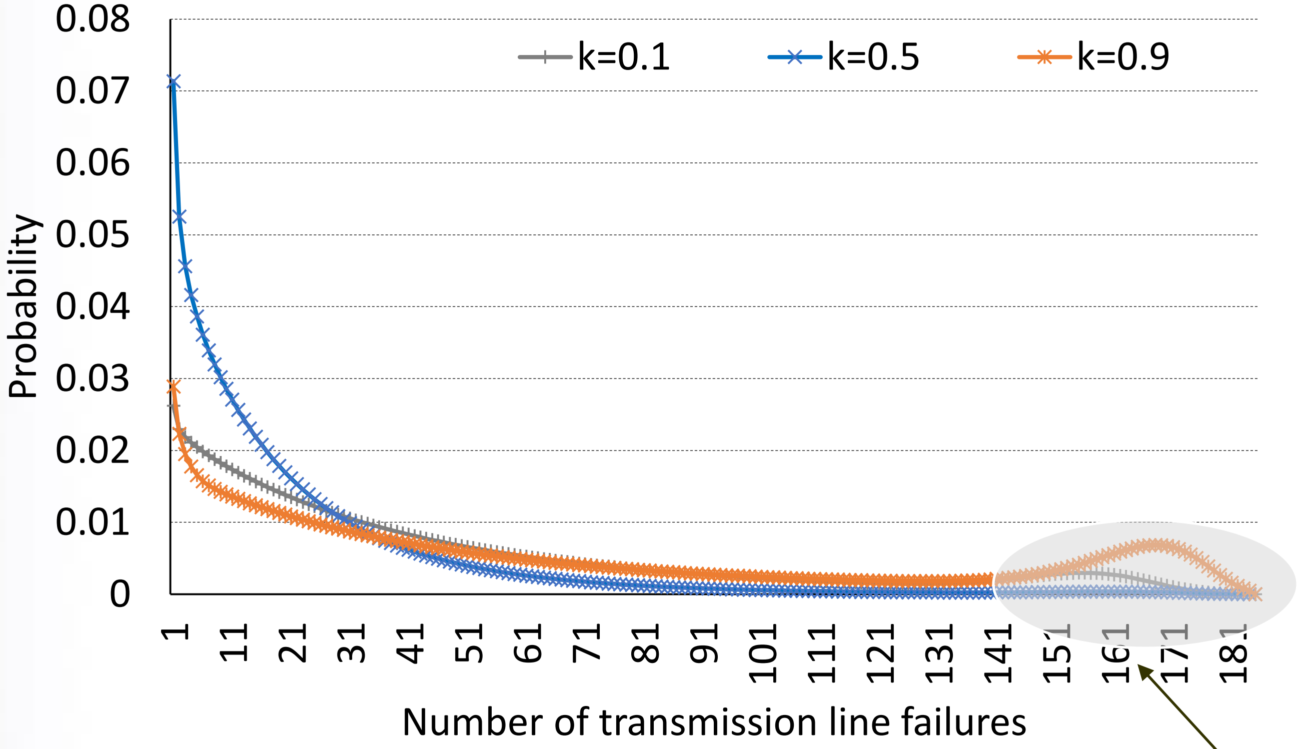
- *Next, we show the capabilities of Markov chain based cascading failure model.*

Cascade stop probability



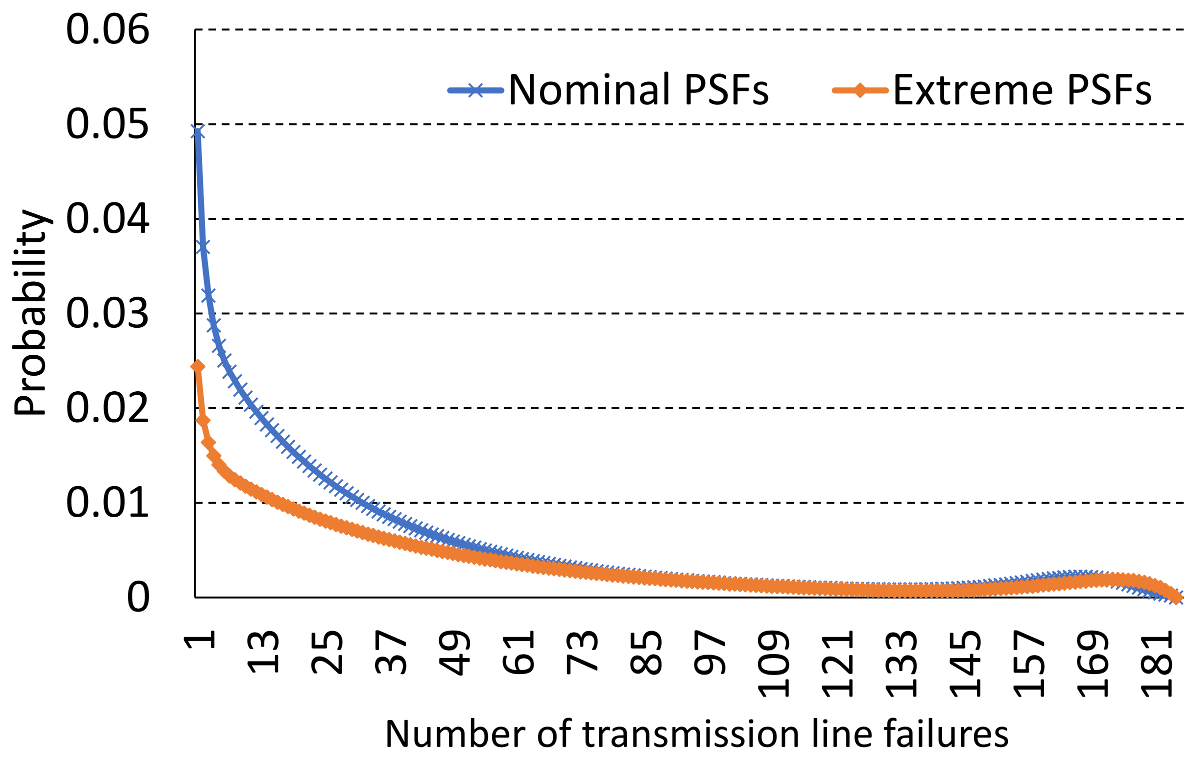
- Lower initial values of cascade-stop probability indicates higher probability of a cascade (for *k* =0.1,0.9) and vice versa (for *k*=0.5).

Distribution of the blackout size



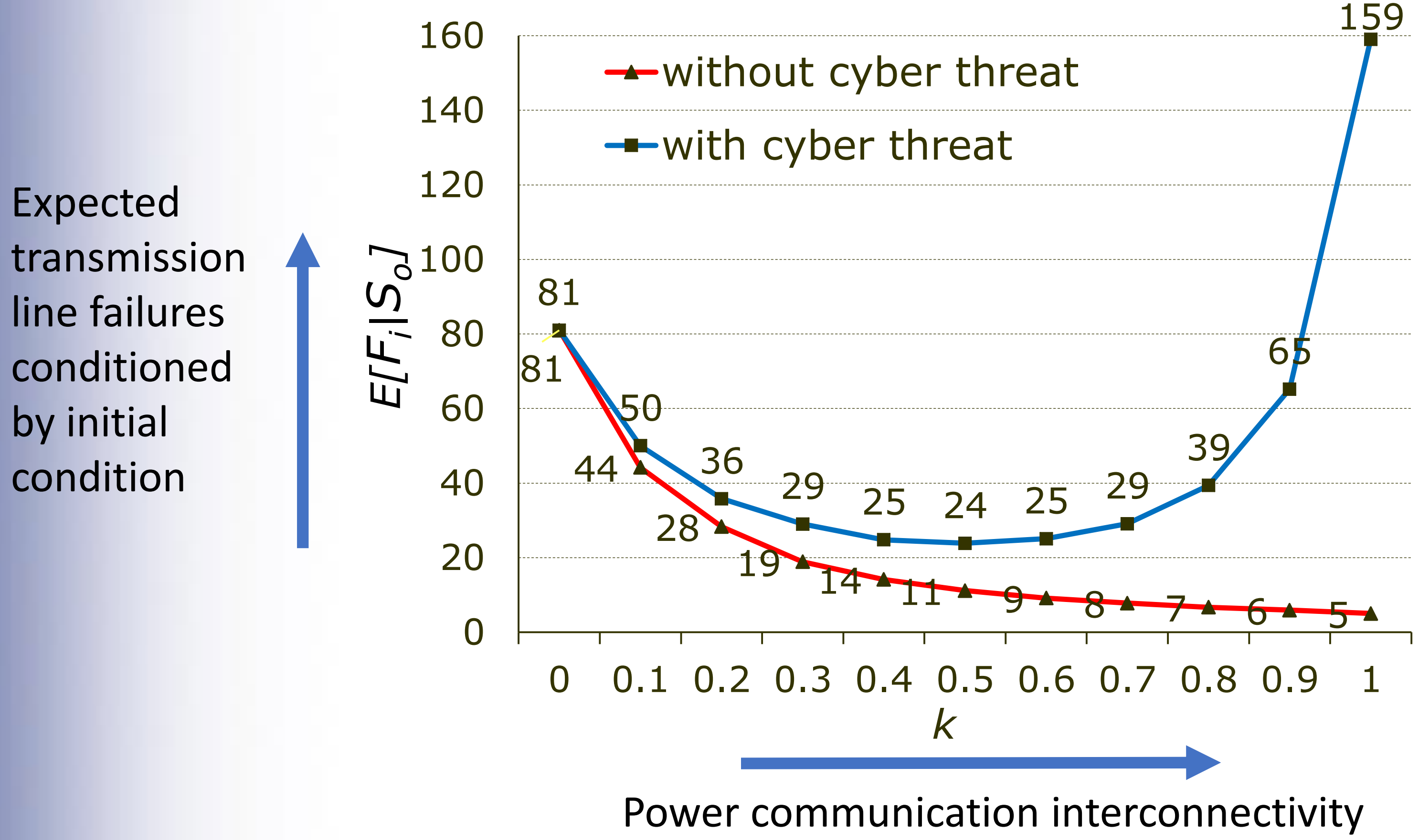
For k = 0.1 and k = 0.9, blackout size distribution shows a **heavy tail**, which indicates a power law distribution as compared to an exponential distribution for k = 0.5.

Distribution of the blackout size



- Distribution of the blackout size for nominal and extreme HEP and k=0.5.
- Average number of transmission-line failures for nominal and extreme HEPs are 24 and 32 lines, respectively.

Optimal power-communication interconnectivity



- Model finds optimal power-communication interconnectivity of enhancing the resilience of the grid against cyber threat.

Conclusions

- A comprehensive 3-layer (power grid, communication, and human response) **Markov chain based analytical cascading failure model** was developed.
- Role of **human operator response** and **cyber threat** on the resilience of the grid was captured.
- This work allows to calculate the **blackout size distribution** analytically.
- Model finds **optimal power-communication interconnectivity** of enhancing the resilience of the grid against cyber threat

Extensions

- We are working on devising **optimal policies** to mitigate cascading failures dynamic load shedding.

Thank you for your time.

Questions?