Likelihood Analysis of Cyber Data Attacks to Power Systems

Yingshuai Hao

Department of Electrical, Computer & System Engineering

Rensselaer Polytechnic Institute

Acknowledgment

- I thank Prof. Meng Wang and Prof. Joe Chow for their instructions.

- This research is supported in part by the ERC Program of NSF and the CURENT Industry Partnership Program, and in part by NYSERDA Grants.

Contents

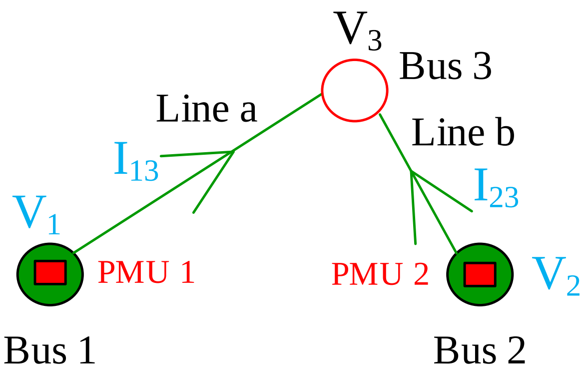
Cyber Data Attacks

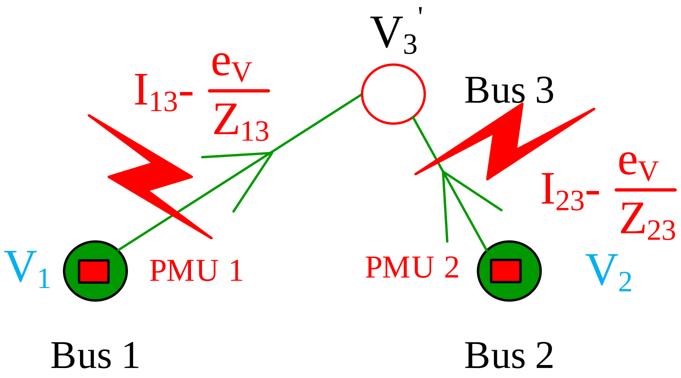
- State Estimation
  - Estimate the operating state of power systems from measurements.
  - Detect and exclude erroneous measurements (bad data) to reduce the estimation error.

- Cyber data attack: first studied by Y. Liu, et al.[1], means:
  - An intruder injects additive errors to multiple measurements.
  - The injected errors could bypass the bad data detector, thus potentially result in significant error in the estimated states.
  - Precondition: the intruder should have sufficient system information.

Cyber Data Attacks

An example of cyber data attacks:





$$\begin{aligned} V_3 &= V_1 - I_{13}Z_{13} \\ &= V_2 - I_{23}Z_{23} \end{aligned}$$

$$\begin{aligned} V_3' &= V_1 - \left(I_{13} - \frac{e_V}{Z_{13}}\right)Z_{13} \\ &= V_2 - \left(I_{23} - \frac{e_V}{Z_{23}}\right)Z_{23} \\ &= V_3 + e_V \end{aligned}$$

Cyber Data Attacks

Existing research on cyber data attacks:

- Identification and protection of a small number of key measurement units [T. Kim, et al. 2011, G. Dan, et al. 2010]
  - The measurements of protected units cannot be changed. Thus the intruder cannot launch cyber data attacks without access to some measurements.
- Detection of cyber data attacks [L. Liu, et al. 2014, H. Sedghi, et al. 2013, M. Wang, et al. 2014]
  - Exploit temporal correlations in the measurements to detected attacks
- The potential financial risks of cyber data attacks [L. Xie, et al. 2011, L. Jia, et al. 2014]
  - Intruders inject errors to change the congestion state of some lines
  - Obtain reward from the resulting change of electricity price

Research Focus

Missing components in the study of cyber data attacks:

- Frequency of data attacks in smart grids during one certain period.
- Likelihood of attacks at a given system state.

Significance to system operators:

- To evaluate the system vulnerability to cyber attacks
- To help system operators defend against cyber data attacks.
  - Determine the buses/lines vulnerable to attacks in the system
  - Evaluate the factors affecting the likelihood of data attacks

We take the first step in the research to modelling and analyzing the likelihood of cyber data attacks.

Problem Setups & Goals

We study from the perspective of intruders, find the optimal attack strategy, and then conduct likelihood analysis.

- **Attack motivation**: financial profit in electricity market from successful attacks.
- **Goal of intruders**: find the optimal attack strategy maximizing the total reward.

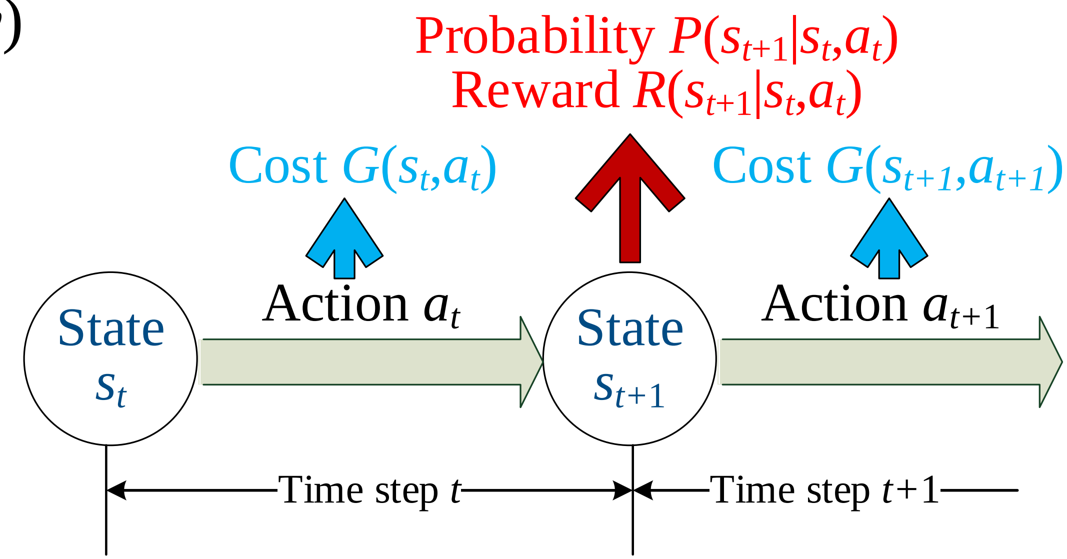
The attack process occurs in a dynamic environment:

- Power system states evolve with time, independent of attacks.
- States of PMUs: evolve with time as well, affected by attack actions.

Problem Formulation

Model the intruder's action process as a **Markov Decision Process**:

(S, A, P, R, γ)



- The optimal attack strategy, a mapping from states to actions, maximizes the expected net reward:

$$E\left[\sum_{t=0}^{T} \gamma^t \left(R(s_{t+1}|s_t,a_t) - G(s_t,a_t)\right)\right]$$

- With the solved optimal attack strategy, attack probability of one bus (line) = **percentage of time when the bus (line) is under attack**

Problem Formulation

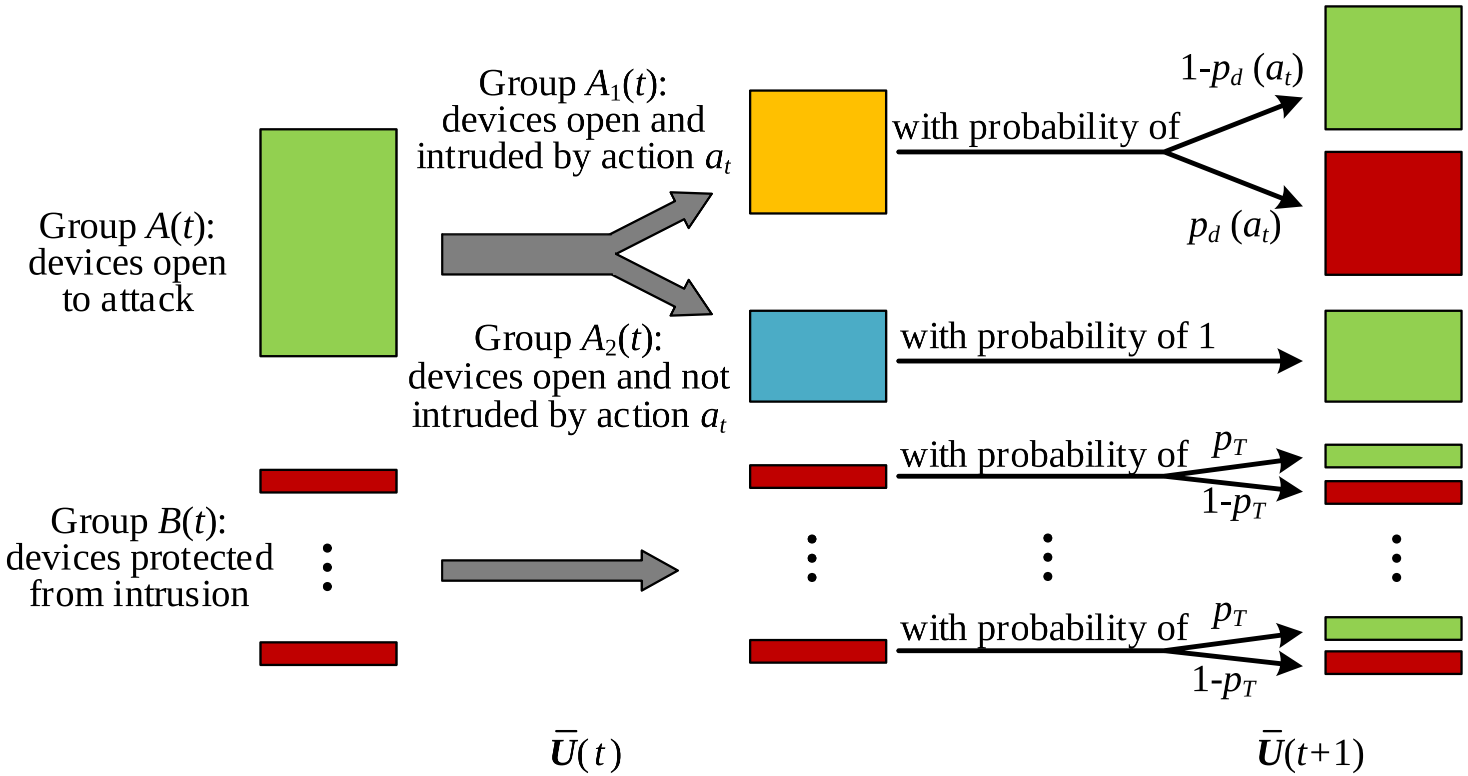
5 tuples of MDP: (S, A, P, R, γ)

- **State *s***: use the bus voltage magnitudes, angles and PMUs' states together. $s = (\bar{V}, \bar{\theta}, \bar{U})$
  - Discrete system states $(\bar{V}, \bar{\theta})$
  - PMU state $\bar{U}$: '0' protected; '1' open to attack
- **Action *a***: set of target buses, injected errors to bus voltage magnitudes and angels
  - Limited resource: the intruder can manipulate the voltage phasors of at most β buses.
  - The attacks can be detected with certain probability, which increases when the injected errors increase.
- **Reward *r***: results from the change of congestion states of lines
- **Action cost**: proportional to the number of PMUs intruded

Problem Formulation

5 tuples of MDP: (S, A, P, R, γ)

- Transition probability of states of PMUs $\overline{U}$:



Problem Formulation

5 tuples of MDP: (S, A, P, R, γ)

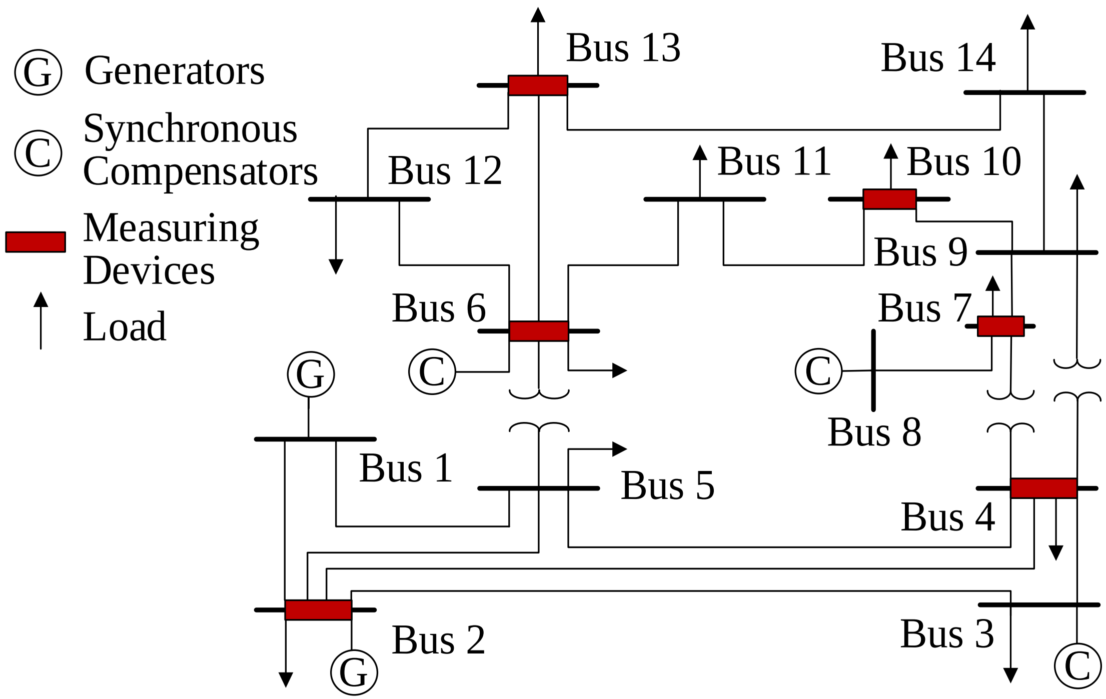
- Transition probability of system states $(\bar{V}, \bar{\theta})$:

We study the intruder's attack actions with two different levels of knowledge about the power system states:

- **Known future system states**
  - The intruder can predict the future system state for a short time.
  - Consider how to act to maximize the expected reward during the period.
  - Formulate as a finite-horizon MDP.
- **Known state transition probabilities of the power system**
  - The intruder models the state evolution of power systems as Markov Chains.
  - The system state transition probability are known to the intruder (e.g. learning from historical data).
  - Consider how to maximize the expected reward for the long run.
  - Formulate as an infinite-horizon MDP.

Simulation

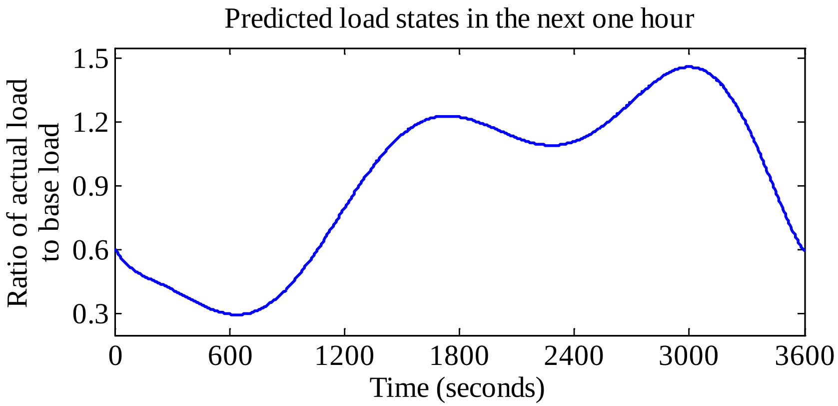
- Power system topology
  - 14 buses, 20 lines, 12 loads and 6 PMUs
  - At each time step, at most two target buses



IEEE 14-Bus Test System

Simulation

- Known future system states:



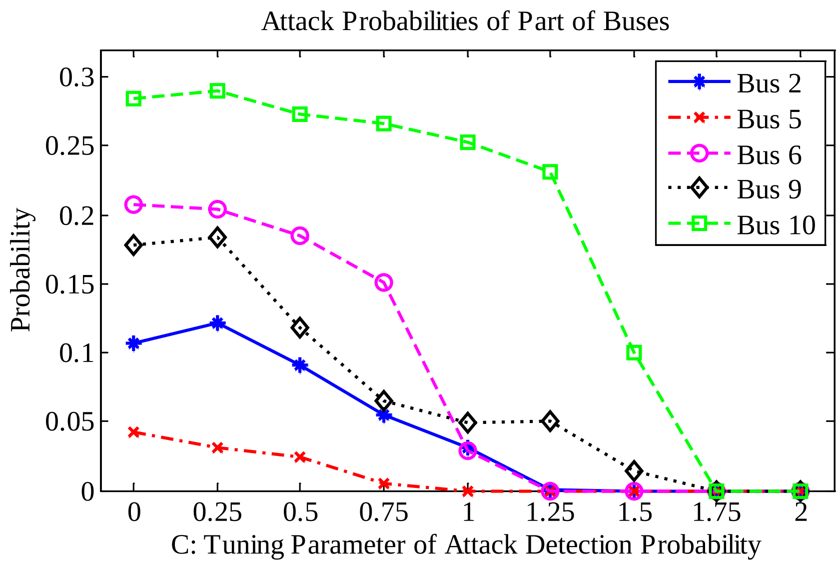
- Predict the system states in the next hour, 720 time steps
- System states are determined from the economic dispatch.

Initial States of PMUs on Bus 2,4,6,7,10,13	Expected attack probability			
	Bus 1	Bus 7	Bus 10	Bus 13
0, 0, 0, 0, 0, 0	5.45%	7.35%	23.10%	3.05%
0, 0, 0, 1, 1, 1	5.45%	7.37%	23.18%	3.05%
1, 1, 1, 1, 1, 1	5.45%	7.40%	23.19%	3.05%

- A slight variation in the expected attack probability of each bus when the initial states of PMUs vary.
- Bus 10 is the most vulnerable bus.

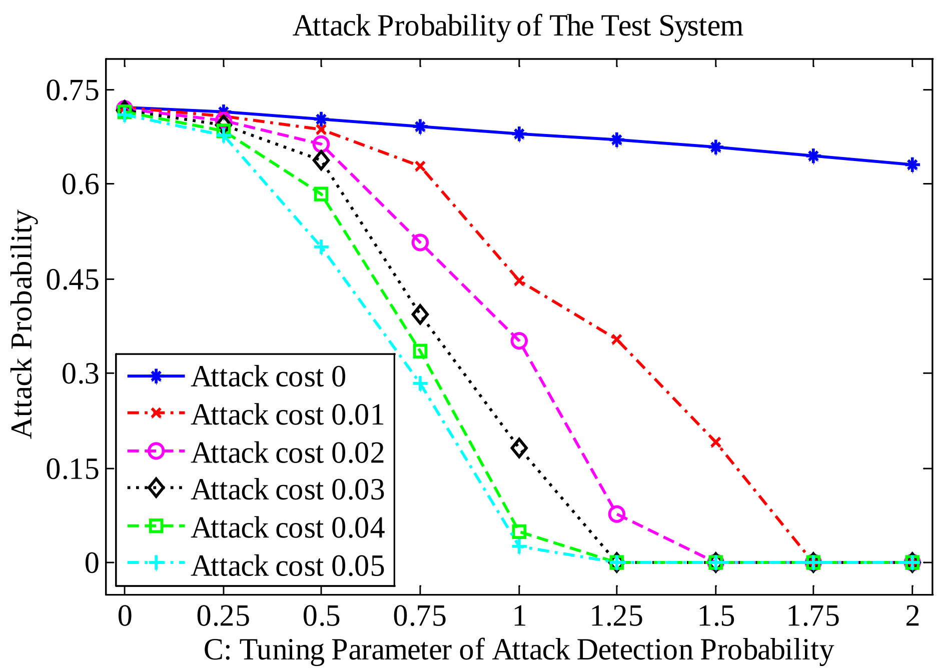
Simulation

- Known the transition probability of system states:



- ***C***: related to the attack detection probability.
  - A larger *C* corresponds to a lower probability of attacks in the system.
  - Parameter C increases, then an attack can be detected with a higher probability. The intruder should be more cautious to launch attacks.
- Bus 10 is the most vulnerable bus.
  - The line connecting bus 9 and 10 has a smaller reactance.
  - The adversary only needs to intrude one PMU to manipulate the state of bus 10.

Simulation



- **Attack cost**: the cost to intruder one PMU.
  - The attack cost increases, then the attack probability of the system decreases.

Simulation

β	P_T	Bus 1	Bus 7	Bus 10
1	0	0.16%	0.16%	0.15%
	0.5	5.46%	7.42%	23.34%
	1	8.03%	12.10%	27.67%
2	0	0.16%	0.16%	0.15%
	0.5	5.45%	7.40%	23.19%
	1	7.98%	19.44%	31.09%
3	0	0.16%	0.16%	0.15%
	0.5	5.16%	6.87%	21.87%
	1	7.59%	10.09%	30.53%

- P_T : the transition probability of PMUs from protected to unprotected.
  - A larger P_T corresponds to a higher attack probability.
- β: the maximal number of buses that the intruder can manipulate their states.
  - In our settings, the order of buses by attack probabilities almost stays the same when β changes.

Conclusion

- Take the first step to analyzing the likelihood of cyber data attacks to power systems.
- Provide the operator with an analytical tool to evaluate the factors contributing to attack defense.
- Characterize the action of an intruder and model the attack action process as a Markov decision process.
- Study the attack strategy and analyze the resulting attack probability with two different levels of intruders' knowledge about power system states.
- Simulate on IEEE 14-bus system to validate our method and discuss four parameters affecting the data attacks.

Reference

[1]. Y. Liu, P. Ning, and M. K. Reiter, “False data injection attacks against state estimation in electric power grids,” in Proceedings of the 16th ACM conference on Computer and communications security, 2009, pp. 21–32.

[2]. T. Kim and H. Poor, “Strategic protection against data injection attacks on power grids,” IEEE Trans. Smart Grid, vol. 2, no. 2, pp. 326–333, 2011.

[3]. G. Dán and H. Sandberg, “Stealth attacks and protection schemes for state estimators in power systems,” in Proc. IEEE International Conference on Smart Grid Communications (SmartGridComm), 2010, pp. 214–219.

[4]. L. Liu, M. Esmalifalak, Q. Ding, V. A. Emesih, and Z. Han, “Detecting false data injection attacks on power grid by sparse optimization,” IEEE Trans. Smart Grid, vol. 5, no. 2, pp. 612–621, 2014.

[5]. H. Sedghi and E. Jonckheere, “Statistical structure learning of smart grid for detection of false data injection,” in Proc. IEEE Power and Energy Society General Meeting (PES), 2013, pp. 1–5.

[6]. M. Wang, P. Gao, S. Ghiocel, J. H. Chow, B. Fardanesh, G. Stefopoulos, and M. P. Razanousky, “Identification of "unobservable" cyber data attacks on power grids,” in Proc. IEEE SmartGridComm, 2014.

[7]. L. Xie, Y. Mo, and B. Sinopoli, “Integrity data attacks in power market operations,” IEEE Trans. Smart Grid, vol. 2, no. 4, pp. 659–666, 2011.

[8]. L. Jia, J. Kim, R. J. Thomas, and L. Tong, “Impact of data quality on real-time locational marginal price,” IEEE Trans. Power Syst., vol. 29, no. 2, pp. 627–636, 2014.

Thank you!

State Estimation

- State variable $x = (V, \theta)$, then the measurement z satisfying $z = h(x) + \omega$, where ω denotes the measurement noise.
- Estimated state

$$\hat{x} = \operatorname{argmin} \left(z - h(x)\right)^T R^{-1} \left(z - h(x)\right).$$

- Bad data detection:

$$\left(z - h(\hat{x})\right)^T R^{-1} \left(z - h(\hat{x})\right) \gtrless \tau$$

Attack Reward

- From the discrete system states, get the **upper and lower bound** of real power of each line. If the congestion state of one line is changed after successful error injection, then we think there is a resulting reward.

- The reward is proportional to the gap between the flow limit and the power bounds with injected errors:

$$r_{ij}(s,a) = \begin{cases} K_{ij} \times \left(P_{ij}^{\min}(\bar{\boldsymbol{V}}', \bar{\boldsymbol{\theta}}') - P_{ij}^{\mathrm{M}}\right) / P_{ij}^{\mathrm{M}}, \\ \ \text{if } P_{ij}^{\min}(\bar{\boldsymbol{V}}', \bar{\boldsymbol{\theta}}') > P_{ij}^{\mathrm{M}} > P_{ij}^{\max}(\bar{\boldsymbol{V}}, \bar{\boldsymbol{\theta}}); \\ K_{ij} \times \left(P_{ij}^{\mathrm{M}} - P_{ij}^{\max}(\bar{\boldsymbol{V}}', \bar{\boldsymbol{\theta}}')\right) / P_{ij}^{\mathrm{M}}, \\ \ \text{if } P_{ij}^{\min}(\bar{\boldsymbol{V}}, \bar{\boldsymbol{\theta}}) > P_{ij}^{\mathrm{M}} > P_{ij}^{\max}(\bar{\boldsymbol{V}}', \bar{\boldsymbol{\theta}}'); \\ 0, \quad \text{otherwise}, \end{cases}$$

Attack Likelihood Analysis

- Attack probability of one bus (line) = the expected number of steps that the bus (line) is under attack during the horizon / the number of total steps in the horizon

- For finite MDPs, we can compute directly. For infinite-horizon MDPs, based on the Law of Large Number, we can compute the distribution probability of each state. Then the attack probability of one bus (line) = the sum of distribution probabilities of states in which the bus (line) is one target bus (line)