Likelihood Analysis of Cyber Data Attacks to Power Systems with Markov Decision Processes

Yingshuai Hao, *Student Member, IEEE,* Meng Wang, *Member, IEEE*, Joe H. Chow, *Fellow, IEEE*

***Abstract*—Cyber data attacks are the worst-case interacting bad data to power system state estimation and cannot be detected by existing bad data detectors. This paper for the first time analyzes the likelihood of cyber data attacks by characterizing the actions of a malicious intruder in a dynamic environment, where power system state evolves with time, and measurement devices could become inaccessible due to detected attacks. This analysis is important for the operator to evaluate the vulnerability of power systems to data attacks. A Markov decision process is proposed to model an intruder's strategy, with the objective to maximize its cumulative reward across time. The optimal attack policy is solved from the intruder's perspective, and the attack likelihood is then analyzed based on the obtained policy. Two attack scenarios are studied to model different knowledge levels of the intruder about the dynamics of power systems. Numerical experiments are conducted on the IEEE 14-bus and 30-bus test systems to study the intruder's attack strategy and analyze the attack probability.**

***Index Terms*—Cyber data attacks, Markov Decision Process, state estimation, power systems.**

I. Introduction

STATE estimation [2] solves for power system states from measurements. Since bad data (erroneous measurements) can result in significant errors in the outcome of state estimation and potentially lead to catastrophic consequences, bad data detection has been extensively studied [3]–[7].

The integration of cyber infrastructures in future smart grids increases the possibility of cyber attacks. Cyber data attacks are viewed as "the worst interacting bad data injected by an adversary" [8], [9]. A malicious intruder with sufficient system configuration information can manipulate multiple measurements simultaneously such that the injected errors cannot be detected by any bad data detector that relies on measurements obtained at a given time instant.

State estimation in the presence of cyber data attacks has attracted much research attention recently [8]–[17]. Since cyber data attacks were considered as undetectable until recently, most efforts have been devoted to studying the requirements to launch a cyber data attack [11], [15] and preventing these attacks by protecting a small number of key measurement units [10], [11], [18]. A few recent work considered the detection of cyber data attacks [13], [14], [19], which exploited abnormal patterns of measurements in the time series to detect attacks.

Because the interacting data attacks can also be detected, a natural question to the intruder is to figure out the optimal attack strategy to maximize its overall benefit as the power system state changes over time. The operator, however, needs to analyze the frequency and likelihood of these attacks so as to take preventive actions or protect highly vulnerable components. Although the interaction of an intruder and an operator for physical infrastructure attacks has been studied through a game-theoretic approach [20], similar analysis is missing for cyber data attacks.

This paper takes the first step to analyzing the likelihood of data attacks and system vulnerability to these attacks through studying the optimal attack strategy of an intruder. Since existing works mostly studied cyber data attacks at a given time instant, there exists no analysis of cyber data attacks when the system state evolves. One contribution of this paper is the development of a general model of an intruder's attack process. This model enables the first mathematical analysis of cyber data attacks in a dynamic setup. In this model, the intruder's objective is to maximize its aggregate reward (e.g., financial benefits, degradation of system stability, etc) over a given period. If an attack is detected by the operator, the intruded measurement units will become inaccessible to intruders, and the corresponding measurements cannot be manipulated[1]. Thus, the intruder's current action affects its available actions and potential benefits in the future. A Markov Decision Process (MDP) [21] is employed to model the intruder's attack decision across time. Two levels of the intruder's knowledge about future power system states are studied in the paper. We consider both the special case that the intruder can predict the future states for a short time and the general case that the intruder has less knowledge and employs a Markov Chain to model the evolvement of the system states. The intruder's action process in these two scenarios are formulated as a finite-horizon MDP and an infinite-horizon MDP respectively. Note that although the parameters of the MDP depend on the system's features and the operating program, the MDP-based approach does not. The MPD-based approach is a general framework to study an intruder's attack process.

The solution to the MDP is a mapping from power system states to the intruder's optimal actions (including which buses to intrude and what errors to inject). The operator can also solve the MPD and compute the attack likelihood based on the obtained attack strategy. The operator can then study the vulnerability of individual components and analyze the impact of various factors (such as detection probability and system transition probabilities) on system vulnerability.

Y. Hao, M. Wang, and J.H. Chow are with the Dept. of Electrical, Computer, and Systems Engineering, Rensselaer Polytechnic Institute, Troy, NY. Email: {haoy2, wangm7, chowj}@rpi.edu.

Partial and preliminary results appeared in [1].

[1] For example, the measurement devices and corresponding data channels will be protected through a combination of encryption, continuous monitoring, separation from the Internet, etc [18].

Numerical experiments demonstrate that the results of the vulnerability analysis are robust to parameter selections of the MPD-problem, the operator's dispatch strategies, and minor inaccuracies in the models to some degree. This property enables the operator to study the vulnerability of the system even with limited knowledge of the intruder's behavior.

The rest of the paper is organized as follows. Section II presents the problem motivation and introduces cyber data attacks and MDPs. The intruder's attack process is formulated as MDPs in Section III. The solutions and likelihood analysis are discussed in Section IV. Numerical experiments on the IEEE 14-bus and 30-bus systems are presented in Section V to illustrate our methods. Section VI concludes the paper.

II. Problem Motivation and Background

A. Cyber Data Attacks in Power Systems

The state of an n-bus power system is represented by $\boldsymbol{x} = (\boldsymbol{V},\ \boldsymbol{\theta})$, where $V_i \in \mathbb{R}$ and $\theta_i \in [-\pi, \pi)$ represent the voltage magnitude and angle of bus i, respectively, and $\boldsymbol{V} = [V_1, ..., V_n]$ and $\boldsymbol{\theta} = [\theta_1, ..., \theta_n]$. Each measurement unit measures some quantities in the system, e.g., the active power flow on a transmission line. Let vector $\boldsymbol{z} \in \mathbb{R}^k$ denote all the measurements, then $\boldsymbol{z} = \mathcal{H}(\boldsymbol{x}) + \boldsymbol{\omega}$, where $\mathcal{H}$ is a set of k functions, and $\boldsymbol{\omega} \in \mathbb{R}^k$ represents the random measurement noise. For example, when line resistances and shunt admittances are ignored, the real power flow from bus i to bus j on line ij is

$$P_{ij} = (X_{ij})^{-1} \cdot V_i \cdot V_j \cdot \sin(\theta_i - \theta_j), \tag{1}$$

where X_{ij} denotes the reactance of line ij.

All the measurements are transmitted to the central operator through the communication network. After collecting $\boldsymbol{z}$, the central operator solves an inverse problem to estimate the system state, denoted by $\hat{\boldsymbol{x}}$, usually through solving a weighted least square optimization problem, i.e.,

$$\hat{\boldsymbol{x}} = \arg\min_{\boldsymbol{x}} (\boldsymbol{z} - \mathcal{H}(\boldsymbol{x}))^T \cdot \boldsymbol{R}^{-1} \cdot (\boldsymbol{z} - \mathcal{H}(\boldsymbol{x})), \tag{2}$$

where $\boldsymbol{R} \in \mathbb{R}^{k \times k}$ is the covariance matrix of measurement noise $\boldsymbol{\omega}$. Bad data in $\boldsymbol{z}$ can be detected if

$$(\boldsymbol{z} - \mathcal{H}(\hat{\boldsymbol{x}}))^T \boldsymbol{R}^{-1} (\boldsymbol{z} - \mathcal{H}(\hat{\boldsymbol{x}})) > \tau, \tag{3}$$

where τ is a prescribed threshold [2].

An intruder with sufficient system information can inject interacting errors to multiple measurements. The attacks can happen during the data sampling period at the measurement devices and/or during the data transmission from the device to the central operator. If the injected additive error vector $\boldsymbol{e_z} \in \mathbb{R}^k$ to the measurements satisfies

$$\boldsymbol{z} + \boldsymbol{e_z} = h(\boldsymbol{x'}) + \boldsymbol{\omega} = h(\boldsymbol{V} + \boldsymbol{e_V}, \boldsymbol{\theta} + \boldsymbol{e_\theta}) + \boldsymbol{\omega}, \tag{4}$$

the operator would obtain a wrong estimate $(\boldsymbol{V} + \boldsymbol{e_V}, \boldsymbol{\theta} + \boldsymbol{e_\theta})$ instead of the actual state $(\boldsymbol{V}, \boldsymbol{\theta})$. Thus, $\boldsymbol{e_V}$ and $\boldsymbol{e_\theta}$ represent the resulting injected errors to state variables $\boldsymbol{V}$ and $\boldsymbol{\theta}$ by injecting errors $\boldsymbol{z}$ to the measurements. These interacting bad data injections $\boldsymbol{e_z}$, referred to as cyber data attacks [9] in this paper, cannot be detected by any bad data detector that only takes measurements at one time instant as the input.

The potential financial risks of cyber data attacks were studied in [22] and [23]. The injected errors can lead to a change of the *congestion pattern*, which is referred to as the set of lines that are estimated to be congested. The locational marginal price (LMP) of the electricity would change accordingly, which results in the finical profits of the intruder.

B. Question to address: likelihood of cyber data attacks

This paper is focused on cyber data attacks that can pass conventional bad data detectors, i.e., satisfy (4). Note that these attacks can still be detected by methods in [13], [14], [19]. The attack objective is quantified through financial benefits in electricity market [22], [23]. Therefore, an attack changes the congestion pattern to gain reward. One can generalize the method here to study other motivations of cyber data attacks by replacing the objective function.

Given a system state, the intruder decides which measurement units to attack and what errors to inject, aiming to maximize the sum of two rewards:

a. The net reward of the current attack.

The intruder obtains a reward if an attack is not detected by the operator and changes the congestion pattern of the power system. The effort to inject an attack is modeled by a "cost". The net reward is the reward minus the cost.

b. The aggregate reward from potential future attacks.

The future reward is affected by the current attack. If an attack is detected, there is no immediate reward, and the operator will protect the affected devices, which in turn limits the future choices of attacks.

The major challenge for an intruder to find the optimal attack strategy results from its limited knowledge of future system states. That includes two aspects:

1. Uncertainty of the future states of measuring devices.

The intruder does not know if an attack would be detected by the operator beforehand. It only has an estimate of the success probability (obtained probably from trials).

2. Uncertainy of the future power system states.

This paper starts with a special case that the intruder can accurately predict the states of the power systems for a short period. Then the analysis is extended to the general case that future power system states are unknown to the intruder. The intruder is assumed to model the state evolvement of power systems as a Markov Chain and estimate the state transition probability from historical data. Note that the system state depends on the operator's control strategy, which is implicitly modeled through state evolvement in this paper. Although the actual power system does not evolve as a Markov Chain, the latter is a reasonable tool for the intruder with limited knowledge to model the system state.

The intruder's decision process is formulated as a Markov Decision Process [21] in this paper. The likelihood of cyber data attacks is analyzed from the optimal attack strategy.

C. Markov Decision Processes (MDPs)

An MDP is defined as a 5-tuple (S, A, R, p, γ): $S = \{s_1, s_2, \dots, s_n\}$ represents the set of system states; A is the set of actions, and each state s has an associated set of available actions $A(s)$. $p(s'|s, a)$ is the probability that the system

TABLE I
NOTATIONS

V_i, θ_i	Magnitude and angle of the estimated voltage phasor of bus i
$\bar{V}_i$, $\bar{\theta}_i$	Discrete states of V_i and θ_i
$\bar{U}_i$	State of the ith measuring device
$\bar{\boldsymbol{V}}^i$, $\bar{\boldsymbol{\theta}}^i$	Vectors of discrete states of voltage magnitude and angle of all buses at state s^i
$\bar{\boldsymbol{U}}^i$	Vector of the states of all measuring devices at state s^i
$\boldsymbol{e_V}$, $\boldsymbol{e_\theta}$	Vectors of injected errors to voltage magnitude and angle of all buses
$R(s'\|s,a)$	Reward after state transits from s to s' under action a
$R(s,a)$	Expected immediate reward from action a at state s
$p(s'\|s,a)$	Transition probability from state s to s' with action a
$G(s,a)$	Total cost to take action a at state s
P_{ij}^M	Real power flow limit on line ij (connecting bus i and bus j)
$P_{ij}^{\max(\min)}$	Upper(lower) bound of line ij's real power estimated from the discrete states of bus voltage phasors
p_T	Probability that an inaccessible device becomes open to attack in the next time step
$\Phi_b(a)$	Set of target buses of which the voltage phasors are manipulated by action a
$\Phi_l(s,a)$	Set of target lines of which the congestion states are changed by action a at state s
$p_d(a)$	Probability that attack a is detected by operators
$p_r(s)$	Stationary distribution probability of state s
$p_b(i)$	Probability that the voltage phasor of bus i is manipulated
p_{sys}	Probability that there exists data attacks in the system
$\Phi_d(a)$	Set of the intruded measuring devices by action a
π^*, $\hat{\pi}$	Optimal and near optimal solutions to an MDP.

transits to state s' after taking action a in state s. $G(s,a)$ is the cost of taking action a at state s. $R(s'|s,a)$ represents the reward when the state transits from s to s' with action a. γ is the discount factor for future rewards. The expected immediate reward from action a at state s is:

$$R(s,a) = \mathbb{E}\left[R(s'|s,a)\right] = \sum_{s'\in S} p(s'|s,a)\cdot R(s'|s,a). \tag{5}$$

The goal is to find the optimal actions that maximize the expected accumulated net rewards as follows

$$\mathbb{E}\left[\sum_{t=0}^{T} \gamma^t \left(R(s_{t+1}|s_t,a_t) - G(s_t,a_t)\right)\right]. \tag{6}$$

When T is finite, the problem is a finite-horizon MDP and γ can be chosen from $[0,1]$. When T is infinite, (6) is an infinite-horizon MDP, and the discount factor γ should be in $[0,1)$, since the value of (6) can be unbounded if $\gamma = 1$.

The MDP problem can be solved exactly by various methods, e.g., dynamic programming and value iteration [21]. The computational complexity depends on the dimensionalities of the state space and the action set. Linear programming with sampled constraints is an efficient method to obtain the near-optimal actions with reduced complexity [24].

III. PROBLEM FORMULATION

The intruder's action process is formulated as an MDP. Two types of MDPs are discussed to model the intruder's different knowledge levels about the dynamics of power system states. The common settings are presented in Section III-A, and the distinct settings are discussed in Section III-B. The notations in this paper are summarized in Table I.

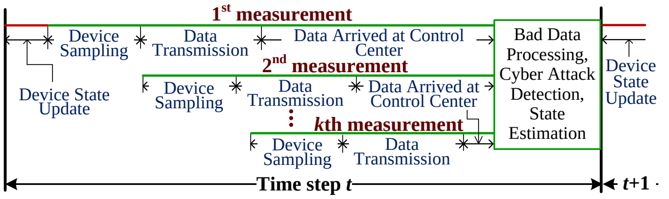


Fig. 1. Event sequence with cyber data attacks. An intruder changes the observations of measuring devices to mislead the operator.

A. Common settings of the formulated MDPs

1) Discrete States and Time Steps: The intruder's estimate of power system states are represented by discrete variables in the formulated MDP. Let n_V and n_θ denote the number of discrete states in voltage magnitudes and angles, respectively. Let $V_i^{\max}$ and $V_i^{\min}$ denote the upper bound and lower bound of V_i, voltage magnitude of bus i, respectively, and $\Delta V_i = V_i^{\max} - V_i^{\min}$. The discrete state of V_i is defined as

$$\bar{V}_i = q/n_V,\ q \in \{1,2,\cdots,n_V\}, \quad \text{if} \tag{7}$$

$$V_i \in \left[V_i^{\min} + (q-1)\cdot\frac{\Delta V_i}{n_V}, V_i^{\min} + q\cdot\frac{\Delta V_i}{n_V}\right). \tag{8}$$

Then given $\bar{V}_i$, we know

$$V_i \in \mathbf{I}_{\bar{V}_i} := \left[V_i^{\min} + \bar{V}_i\cdot\Delta V_i - \tfrac{\Delta V_i}{n_V}, V_i^{\min} + \bar{V}_i\cdot\Delta V_i\right). \tag{9}$$

Similarly, let $\theta_i^{\max}$ and $\theta_i^{\min}$ denote the upper bound and lower bound of θ_i, respectively, and $\Delta\theta_i = \theta_i^{\max} - \theta_i^{\min}$. The discrete state of θ_i is

$$\bar{\theta}_i = q/n_\theta,\ q \in \{1,2,\cdots,n_\theta\}, \quad \text{if} \tag{10}$$

$$\theta_i \in \left[\theta_i^{\min} + (q-1)\cdot\frac{\Delta\theta_i}{n_\theta}, \theta_i^{\min} + q\cdot\frac{\Delta\theta_i}{n_\theta}\right). \tag{11}$$

Given $\bar{\theta}_i$, we have

$$\theta_i \in \mathbf{I}_{\bar{\theta}_i} := \left[\theta_i^{\min} + \bar{\theta}_i\cdot\Delta\theta_i - \tfrac{\Delta\theta_i}{n_\theta}, \theta_i^{\min} + \bar{\theta}_i\cdot\Delta\theta_i\right). \tag{12}$$

$\bar{U}_j$ denotes the state of the jth measuring device. $\bar{U}_j$ is '1' if the device is open to attack, i.e. an intruder can change partial or all measurements of that device. '0' means the device is inaccessible for attacks. An intruder might observe the measurements but cannot change the measurements.

Each time step of a discrete-time MDP corresponds to the instant of state estimation. The sampling rate of measuring devices can be higher than the frequency of the state estimation, as is shown in Fig. 1.

The state of an MDP includes bus voltage magnitudes, angles, and the states of measuring devices together. Suppose a power system has n buses and m measuring devices. Let

$$\bar{\boldsymbol{V}}(t) = [\bar{V}_1(t),\cdots,\bar{V}_n(t)], \bar{\boldsymbol{\theta}}(t) = [\bar{\theta}_1(t),\cdots,\bar{\theta}_n(t)], \tag{13}$$

$$\text{and } \bar{\boldsymbol{U}}(t) = [\bar{U}_1(t),\cdots,\bar{U}_m(t)] \tag{14}$$

denote discrete states of voltage magnitudes, angles, and measuring devices at time step t, respectively, then the state s_t at time step t of an MDP is

$$s_t = \left[\bar{\boldsymbol{V}}(t), \bar{\boldsymbol{\theta}}(t), \bar{\boldsymbol{U}}(t)\right]. \tag{15}$$

2) Actions: An attack can lead to wrong estimates of the voltages of some buses, referred to as *target buses*. Let Φ_b denote the set of target buses. $|\cdot|$ denotes the cardinality of a set. We assume at each time step the intruder can affect at most β target buses due to its resource constraints, i.e., $|\Phi_b| \leq \beta$. The intruder has at most $\sum_{i=0}^{\beta} \binom{n}{i}$ choices of the target buses.

Let e_{V_i} and e_{θ_i} denote the resulting injected errors to the voltage magnitude and angle of bus i respectively, when additive errors $\boldsymbol{e_z}$ are injected to the measurements. To pass bad data detectors, $\boldsymbol{e_V}$, $\boldsymbol{e_\theta}$, and $\boldsymbol{e_z}$ should satisfy (4). Since we consider discrete system states, e_{V_i} and e_{θ_i} are multiples of $\frac{\Delta V_i}{n_V}$ and $\frac{\Delta \theta_i}{n_\theta}$ respectively. There are at most $n_V \cdot n_\theta$ choices to manipulate the state of one target bus. Note that $V_i + e_{V_i}$ and $\theta_i + e_{\theta_i}$ should still belong to $\left[V_i^{\min}, V_i^{\max}\right]$ and $\left[\theta_i^{\min}, \theta_i^{\max}\right]$ respectively.

An *action* is a triplet $a = \{\Phi_b(a), \boldsymbol{e_V}(a), \boldsymbol{e_\theta}(a)\}$. $p_d(a)$ denotes the intruder's estimate of the probability that an action a is detected by the network operator. Since $p_d(a)$ depends on the specific detection method (e.g., [13], [14], [19]) and generally increases when the injected errors increase, we propose to quantify $p_d(a)$ by a general function

$$p_d(a) = 1 - \exp\left(-C \cdot \sum_{i=1}^{n} \left(\frac{|e_{V_i}|}{\Delta V_i} + \eta \frac{|e_{\theta_i}|}{\Delta \theta_i}\right)\right), \qquad (16)$$

where a nonnegative constant C depends on the detection method, and the positive constant η is the weighting factor of the errors in the magnitudes and angles. Intuitively, a larger C means a higher detection probability.

At a given state s, some measuring devices may be inaccessible to the intruder and in turn limits the number of available actions. An action is available at state s if and only if for every nonzero entry in its corresponding injected error vector $\boldsymbol{e_z}$, the corresponding measurement device is open to attack.

3) Rewards and Costs: An intruder obtains a reward r_{ij} from line ij if and only if the attack is undetected and changes the estimated congestion state of line ij[2]. Given discrete states ($\bar{\boldsymbol{V}}$,$\bar{\boldsymbol{\theta}}$), the real power flow of line ij can be estimated by upper and lower bounds, denoted by $P_{ij}^{\max}(\bar{\boldsymbol{V}}, \bar{\boldsymbol{\theta}})$ and $P_{ij}^{\min}(\bar{\boldsymbol{V}}, \bar{\boldsymbol{\theta}})$ respectively. From (1), we have

$$P_{ij}^{\min}(\bar{\boldsymbol{V}}, \bar{\boldsymbol{\theta}}) = \tfrac{1}{X_{ij}} \inf_{V_i \in \mathbf{I}_{\bar{V}_i}} V_i \cdot \inf_{V_j \in \mathbf{I}_{\bar{V}_j}} V_j \cdot \inf_{\substack{\theta_i \in \mathbf{I}_{\bar{\theta}_i} \\ \theta_j \in \mathbf{I}_{\bar{\theta}_j}}} |\theta_i - \theta_j|, \quad (17)$$

$$P_{ij}^{\max}(\bar{\boldsymbol{V}}, \bar{\boldsymbol{\theta}}) = \tfrac{1}{X_{ij}} \sup_{V_i \in \mathbf{I}_{\bar{V}_i}} V_i \cdot \sup_{V_j \in \mathbf{I}_{\bar{V}_j}} V_j \cdot \sup_{\substack{\theta_i \in \mathbf{I}_{\bar{\theta}_i} \\ \theta_j \in \mathbf{I}_{\bar{\theta}_j}}} |\theta_i - \theta_j|, \quad (18)$$

where $\mathbf{I}_{\bar{V}_i}, \mathbf{I}_{\bar{\theta}_i}$ are defined in (9)-(12).

r_{ij} is defined to be proportional to the gap between the line flow limit, denoted by P_{ij}^{M}, and the estimated power bounds:

$$r_{ij}(s,a) = \begin{cases} K_{ij} \cdot \left(P_{ij}^{\min}(\bar{\boldsymbol{V}}', \bar{\boldsymbol{\theta}}') - P_{ij}^{\mathrm{M}}\right) / P_{ij}^{\mathrm{M}}, \\ \quad \text{if } P_{ij}^{\min}(\bar{\boldsymbol{V}}', \bar{\boldsymbol{\theta}}') > P_{ij}^{\mathrm{M}} > P_{ij}^{\max}(\bar{\boldsymbol{V}}, \bar{\boldsymbol{\theta}}); \\ K_{ij} \cdot \left(P_{ij}^{\mathrm{M}} - P_{ij}^{\max}(\bar{\boldsymbol{V}}', \bar{\boldsymbol{\theta}}')\right) / P_{ij}^{\mathrm{M}}, \\ \quad \text{if } P_{ij}^{\min}(\bar{\boldsymbol{V}}, \bar{\boldsymbol{\theta}}) > P_{ij}^{\mathrm{M}} > P_{ij}^{\max}(\bar{\boldsymbol{V}}', \bar{\boldsymbol{\theta}}'); \\ 0, \quad \text{otherwise}, \end{cases} \qquad (19)$$

where K_{ij} is the reward weight of line ij and assumed to be constants and independent of system states in this paper for simplicity. $(\bar{\boldsymbol{V}}', \bar{\boldsymbol{\theta}}')$ is the resulting estimates with injected errors $\boldsymbol{e_V}(a)$ and $\boldsymbol{e_\theta}(a)$,

$$\bar{V}_i' = \bar{V}_i + \frac{e_{V_i}(a)}{\Delta V_i}, \ \bar{\theta}_i' = \bar{\theta}_i + \frac{e_{\theta_i}(a)}{\Delta \theta_i}. \qquad (20)$$

Let $\Phi_l(s,a)$ denote the set of lines of which the congestion states are changed by action a. The expected immediate reward from action a at state s is:

$$R(s,a) = (1 - p_d(a)) \cdot \sum_{ij \in \Phi_l(s,a)} r_{ij}(s,a). \qquad (21)$$

The cost to intrude an accessible device is assumed fixed and known, denoted by g_u. Let $\Phi_d(a)$ denote the smallest set of the intruded devices to achieve action a. The attack cost is

$$G(s,a) = g_u \cdot |\Phi_d(a)|. \qquad (22)$$

4) State Transition of Measuring Devices: The state transition of measuring devices is illustrated in Fig. 2. Given $\bar{\boldsymbol{U}}(t)$ and a_t, devices are divided into three groups.

$A_1(t)$ includes the devices that are accessible at time t and intruded by action a_t. At time $t+1$, they will stay accessible if the attack is not detected, but they will become inaccessible if the attack is detected by the operator.

$A_2(t)$ consists of the accessible devices that are not intruded by action a_t. They will stay accessible at time $t+1$.

$B(t)$ contains all the inaccessible devices at time t. In order to model the scenarios that an intruder might be able to hack protected devices as its intelligence improves, we assume each device in $B(t)$ will become accessible independently at time $t+1$ with a fixed probability p_T. Intuitively, a smaller p_T indicates that a device is likely to stay inaccessible for a longer period of time. When $p_T = 0$, the devices will stay inaccessible forever.

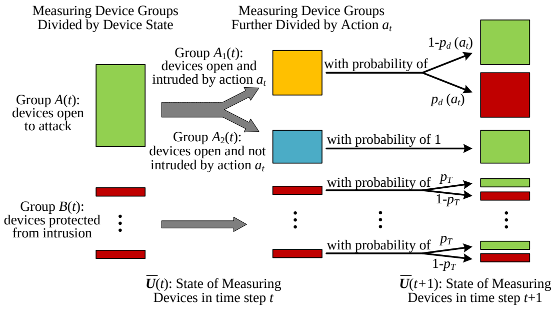

Measuring Device Groups
Divided by Device State
Measuring Device Groups
Further Divided by Action a_t
Group $A(t)$: devices open to attack
Group $A_1(t)$: devices open and intruded by action a_t
Group $A_2(t)$: devices open and not intruded by action a_t
Group $B(t)$: devices protected from intrusion
with probability of
1-p_d (a_t)
p_d (a_t)
with probability of 1
with probability of
p_T
1-p_T
with probability of
p_T
1-p_T
$\bar{\boldsymbol{U}}(t)$: State of Measuring Devices in time step t
$\bar{\boldsymbol{U}}(t+1)$: State of Measuring Devices in time step t+1

Fig. 2. State transition diagram of measuring devices. Green blocks denote the accessible devices; red blocks denote the inaccessible devices; the orange block denotes the set of accessible devices that are intruded by action $a(t)$; the blue block denotes the set of accessible devices that are not intruded by action $a(t)$.

In this case, if k_1 devices of $B(t)$ remain inaccessible, and k_2 devices of $B(t)$ become open to attack independently in $\bar{\boldsymbol{U}}(t+1)$ for any integer k_1 and k_2 such that $k_1 + k_2 = |B(t)|$, then the transition probability from $\bar{\boldsymbol{U}}(t)$ to $\bar{\boldsymbol{U}}(t+1)$ after

[2] One can study other attack motivations by changing the definition of the reward. For example, a reward function could be the decrease of the system security margin, or the decrease of some bus voltage from 1 p.u..

taking action a_t is:

$$p(\bar{\boldsymbol{U}}(t+1)|\bar{\boldsymbol{U}}(t),a_t)=\begin{cases}(1-p_d(a_t))\cdot p_T^{k_1}\cdot(1-p_T)^{k_2},\\ \text{if } a_t \text{ is not detected}, \forall k_1+k_2=|B(t)|;\\ p_d(a_t)\cdot p_T^{k_1}\cdot(1-p_T)^{k_2},\\ \text{if } a_t \text{ is detected}, \forall k_1+k_2=|B(t)|;\\ 0, \quad \text{otherwise}.\end{cases} \tag{23}$$

where $p_d(a_t)$ and p_T are scalers defined in (16) and the previous paragraph.

B. Distinct attack scenarios and formulated MDPs

We assume the system state evolves independently of the data attack actions in a short period of time. The reason is twofold. First, the data acquisition rate is much higher than the change of dispatch decisions. Second, an intruder might not have enough intelligence to predict the reactions of the operator to drastic attacks. We consider two levels of the intruders' knowledge about how power system state evolves.

1) Scenario I – Known future states of the power system: The intruder can accurately predict the discrete system states for some time. This happens when the system is stationary or follows a repetitive pattern. Thus, bus voltage magnitudes and angles during the predicted period are deterministic functions of time t, represented by $(\bar{\boldsymbol{V}}(t), \bar{\boldsymbol{\theta}}(t))$. Then, the state transition is fully determined by the intruder's action and devices' states, i.e.,

$$\begin{aligned}&p(\bar{\boldsymbol{V}}(t+1),\bar{\boldsymbol{\theta}}(t+1),\bar{\boldsymbol{U}}(t+1)|\bar{\boldsymbol{V}}(t),\bar{\boldsymbol{\theta}}(t),\bar{\boldsymbol{U}}(t),a_t)\\ =&p(\bar{\boldsymbol{U}}(t+1)|\bar{\boldsymbol{U}}(t),a_t).\end{aligned} \tag{24}$$

The number of states is reduced to $2^m \cdot T$, where m is the number of deployed measuring devices, and T is the total number of time steps. Since the intruder aims to maximize its expected cumulative reward in (6) during the prediction period, the problem can be formulated as a finite-horizon MDP.

2) Scenario II – Known state transition probabilities of the power system: The intruder does not know the future system states but can employ a Markov Chain to model the state evolution of the power system. The transition probabilities of system states can be estimated from historical data. Let N denote the number of states of the power system, then the total number of states in the MDP problem is $N \cdot 2^m$. The system transition probability from s^i to s^j with action a is:

$$\begin{aligned}p(s^j|s^i,a)&=p(\bar{\boldsymbol{V}}^j,\bar{\boldsymbol{\theta}}^j|\bar{\boldsymbol{V}}^i,\bar{\boldsymbol{\theta}}^i,a)\cdot p(\bar{\boldsymbol{U}}^j|\bar{\boldsymbol{V}}^i,\bar{\boldsymbol{\theta}}^i,\bar{\boldsymbol{U}}^i,a)\\ &=p(\bar{\boldsymbol{V}}^j,\bar{\boldsymbol{\theta}}^j|\bar{\boldsymbol{V}}^i,\bar{\boldsymbol{\theta}}^i,a)\cdot p(\bar{\boldsymbol{U}}^j|\bar{\boldsymbol{U}}^i,a),\end{aligned} \tag{25}$$

where $p(\bar{\boldsymbol{V}}^j,\bar{\boldsymbol{\theta}}^j|\bar{\boldsymbol{V}}^i,\bar{\boldsymbol{\theta}}^i,a)$ is the intruder's estimation on the transition probability from system state $(\bar{\boldsymbol{V}}^i,\bar{\boldsymbol{\theta}}^i)$ to $(\bar{\boldsymbol{V}}^j,\bar{\boldsymbol{\theta}}^j)$ under attack a. The horizon T of the MDP is infinite here.

C. A small example to illustrate the problem formulation

The problem formulation is illustrated on a small system in Fig. 3. For each line, the power limit is 1.3 per unit (p.u.), and the reactance is 0.04 p.u.. Each bus voltage magnitude has 2 discrete states. State 1 is 1.00~1.03 p.u., and state 2 is 1.03~1.06 p.u.. Each bus voltage angle has five states with a resolution of 0.2°. The allowable ranges for voltage angles of bus 1, 2 and 3 are $-0.5°$~$0.5°$, $-0.7°$~$0.3°$ and $-3.4°$~$-2.4°$, respectively. The load has 2 states, and the corresponding discrete system states are shown in Table II.

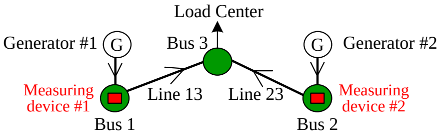


Fig. 3. A simple example of power network

TABLE II
DISCRETE BUS STATES UNDER ALL LOAD STATES

Load State	Discrete States of Bus Voltage Mangitudes and Angles		
	Bus 1	Bus 2	Bus 3
1	2/2, 3/5	2/2, 3/5	1/2, 5/5
2	2/2, 3/5	2/2, 2/5	1/2, 1/5

The congestion state of each line can be calculated from (17) and (18). Take the line 23 with load state 2 as an example. From the discrete states, we know

$$\begin{aligned}&V_2 \in [1.03, 1.06)\,,\ \ \theta_2 \in [-0.5°, -0.3°)\,;\\ &V_3 \in [1.00, 1.03)\,,\ \ \theta_3 \in [-3.4°, -3.2°)\,;\\ &\inf|\theta_2-\theta_3| = 2.7°,\ \sup|\theta_2-\theta_3| = 3.1°;\\ &P_{23}^{\max} = 0.04^{-1}\cdot 1.06\cdot 1.03\cdot \sin(3.1°) = 1.47 > 1.3,\\ &P_{23}^{\min} = 0.04^{-1}\cdot 1.03\cdot 1.00\cdot \sin(2.7°) = 1.21 < 1.3.\end{aligned}$$

In this case, the congestion state of line 23 cannot be determined. Hence we do not consider any reward from line 23. Following this method, line 13 and 23 are uncongested under load state 1, and line 13 is congested under load state 2.

Then all the available actions and the corresponding rewards can be determined. A simple case is provided here that an intruder injects error $(0, -0.6°)$ to the voltage phasor of bus 3 when the load is at state 1.

$$\begin{aligned}&V_3' \in [1.00, 1.03)\,, \theta_3' \in [-3.2°, -3.0°)\,, \inf|\theta_1-\theta_3'| = 2.9°,\\ &P_{13}^{\min} = 0.04^{-1}\cdot 1.03\cdot 1.00\cdot \sin(2.9°) = 1.303 > 1.3.\end{aligned}$$

With the injected error, line 13 becomes congested, and the resulting reward r_{13} is $K_{13}\cdot(1.303-1.3) = 0.003K_{13}$. All the available actions and the corresponding rewards when the number of target buses $\beta = 1$ are shown in Table III.

TABLE III
ALL AVAILABLE ACTIONS AND CORRESPONDING REWARDS WHEN β=1

Load State	Target Bus	Target Lines	Injected Errors e_{V_i}, e_{θ_i}	Resulting Reward $r_{13} + r_{23}$
1	3	13	0, $-0.6°$	$0.003K_{13}$
	3	13	0.03 p.u., $-0.6°$	$0.042K_{13}$
	3	13,23	0, $-0.8°$	$0.093K_{13} + 0.003K_{23}$
	3	13,23	0.03 p.u., $-0.8°$	$0.134K_{13} + 0.042K_{23}$
2	3	13	0, 0.8°	$0.014K_{13}$

The state transition of devices and the transition probability can be determined from (16) and (23). Take the first action in Table III for example, the attack detection probability is $1-\exp(-\frac{3}{5}C\eta)$. In the next step, the measuring devices on Bus 1 and 2 are both protected with probability $1-\exp(-\frac{3}{5}C\eta)$ and both open with probability $\exp(-\frac{3}{5}C\eta)$.

We further consider to the case that $\beta = 2$. Part of the available actions in this case are shown in Table IV.

TABLE IV
PART OF THE AVAILABLE ACTIONS AND CORRESPONDING REWARDS WHEN $\beta = 2$

Load State	Target Buses	Target Lines	Injected Errors e_{V_i}, e_{θ_i}	Resulting Reward $r_{13} + r_{23}$
1	1, 3	13	0, 0.2°; 0, −0.4°	$0.003K_{13}$
	2, 3	13, 23	0, 0.4°; 0, −0.6°	$0.003K_{13}$ $+0.393K_{23}$
2	1, 3	13	0, −0.4°; 0, 0.4°	$0.014K_{13}$
	1, 3	13	0, −0.2°; 0, 0.8°	$0.109K_{13}$

IV. ATTACK PROBABILITY ANALYSIS BY SOLVING MDPS

Although parameters like p_d, p_T, and $p(s_{t+1}|s_t, a_t)$ depend on the operating programs of the system, the MDP-based approach is general and does not depend on the system operation. From an intruder's perspective, it solves the MDP to obtain the optimal attack strategy offline. In the attack process, it first estimates system states from full or partial measurements and then picks the corresponding optimal action accordingly. From the operator's perspective, it can compute the attack likelihood of components in the system based on the MDP solution. It can then take preventive actions to protect the most vulnerable components.

Note that we assume in the attack process, an intruder has access to a sufficient number of measurements to determine the system state. Thus, it only needs to decide which measurements to attack at each time instant. If it can only observe partial measurements and further needs to decide which measurements to observe at each time instant, the problem could be formulated as a Partially Observable Markov Decision Process (POMDP) [25]. We do not follow this direction because an intruder might not have sufficient resource to solve the much more complicated POMDP problem. Moreover, as shown in the later numerical experiments (Section V-D, E), the results of the analysis of the attack likelihood almost stay the same if an intruder's estimation of system state has minor inaccuracies. Thus, the MDP solution is sufficient for the operator to evaluate the system vulnerability.

A. Background of MDP solutions

In an MDP, a policy π is a mapping $\pi : S \mapsto A$, where $\pi(s)$ is the action taken at state s. We define $W_\pi(s)$ as the expected cumulative net reward by starting from state s till terminal time T and following policy π,

$$W_\pi(s) = \mathbb{E}\left[\sum_{t=\tau}^{T} \gamma^{t-\tau}(R(s_{t+1}|s_t, \pi(s_t)) - G(s_t, \pi(s_t)))\middle| s_\tau = s\right], \quad (26)$$

where τ is the first time step when state s appears.

$W^*(s)$ is the value of state s, which is defined as the maximal cumulative reward starting from state s. Then

$$\begin{aligned} W^*(s) &= \max_{\pi\in\Pi} W_\pi(s) \\ &= \max_{a\in A(s)} (R(s,a) - G(s,a) + \gamma \sum_{s'\in S} p(s'|s,a) \cdot W^*(s')), \end{aligned} \quad (27)$$

where Π is the set of all available policies. The optimal policy that achieves the maximum in (27) is denoted as π^*. The optimal action $\pi^*(s)$ at state s is defined as

$$\arg\max_{a\in A(s)}(R(s,a) - G(s,a) + \gamma \sum_{s'\in S} p(s'|s,a) \cdot W^*(s')). \quad (28)$$

B. Attack probability analysis in scenario I

The formulated finite-horizon MDP can be solved by backward dynamic programming [21]. The values of states after terminal step T are zeros, since no further attacks are considered. The value of states at time T can be computed as

$$W^*(s_T) = \max_{a_T\in A(s_T)} (R(s_T, a_T) - G(s_T, a_T)). \quad (29)$$

Then we can follow (27) to compute the value of states at time step $t = T-1, \cdots, 1$ sequentially after computing the state values at time step $t+1$.

$Z_i(s_t)$ is defined as the expected number of time steps during which bus i is under attack from step t to terminal step T with the initial state of s_t. With the optimal attack policy π^* determined from (28), we have

$$Z_i(s_t) = \mathbb{1}_{[i\in\Phi_b(\pi^*(s_t))]} + \sum_{s_{t+1}} p(s_{t+1}|s_t, \pi^*(s_t)) \cdot Z_i(s_{t+1}), \quad (30)$$

where $\mathbb{1}_{[\mathbb{A}]}$ is an indicator function that takes value '1' if event $\mathbb{A}$ happens and takes value '0' otherwise.

Since no further attacks after time step T are considered, $Z_i(s_T) = \mathbb{1}_{[i\in\Phi_b(\pi^*(s_T))]}$. Thus $Z_i(s_0)$ can be computed recursively following (30). The attack probability of bus i is defined as the ratio of $Z_i(s_0)$ to the total number of steps T.

C. Attack probability analysis in scenario II

1) Solution of the formulated infinite-horizon MDP

Considering the computational complexity to solve an MDP exactly [26], a near-optimal policy is determined with approximate linear programming [24]. State value $W^*(s)$ is approximated by a linear combination of K predefined basis functions $\mathbf{y}_k \in \mathbb{R}^{|S|}$, $k = 1, ..., K$, where K is much less than $|S|$. The goal is to find the weight vector $d \in \mathbb{R}^K$ such that $W^*(s) \approx \sum_{k=1}^{K} \mathbf{y}_k(s) d_k = Y(s)d$, where $Y = [\mathbf{y}_1, \mathbf{y}_2, \cdots, \mathbf{y}_K]$. Moreover, the constraints in the LP are sampled and relaxed to further simplify the computation [24], [27]. The ALP method computes the near-optimal policy $\hat{\pi}$ through solving the following optimization problem:

$$\begin{aligned} \min_{\substack{d\in\mathbb{R}^K \\ z(s)}} & \sum_{s\in\Psi(s)} c(s)Y(s)d + \lambda z(s) \\ \text{s.t. } & z(s) \geq -Y(s)d + R(s,a) - G(s,a) \\ & \quad + \gamma \sum_{s'} P(s'|s,a) \cdot Y(s')d, \ \forall a \in A(s), \\ & z(s) \geq 0, \ \forall s \in \Psi(s), \end{aligned} \quad (31)$$

where $c(s)$ is the state-relevance weight, $z(s)$ denotes the penalty of violating a constraint, λ is a positive weight, $\Psi(s)$ is the set of sampled states. The states are sampled uniformly in this paper. Once d is computed through (31), $\hat{\pi}(s)$ can be determined by (28).

2) Attack probability analysis

The stationary distribution $p_r(s)$ of state s can be obtained from the following equation:

$$p_r(s^i) = \sum_{s^j\in S} p(s^i|s^j, \hat{\pi}(s^j)) \cdot p_r(s^j), \ \forall s^i \in S, \quad (32)$$

Note that $\sum_{s^i\in S} p_r(s^i) = 1$. Then the attack probability of bus i, denoted by $p_b(i)$, can be calculated as

$$p_b(i) = \sum_{s \in S} \mathbb{1}_{i \in \Phi_b(\hat{\pi}(s))} \cdot p_r(s). \tag{33}$$

The computational complexity depends on the size of the state space, which is $N \cdot 2^m$. It could be time-consuming in large power systems.

The computational time can be reduced in the case that the transition probability from any system state $(\bar{\boldsymbol{V}}^j, \bar{\boldsymbol{\theta}}^j)$ to state $(\bar{\boldsymbol{V}}^i, \bar{\boldsymbol{\theta}}^i)$ is equal and given, denoted by $q(\bar{\boldsymbol{V}}^i, \bar{\boldsymbol{\theta}}^i)$. One can easily verify that $q(\bar{\boldsymbol{V}}^i, \bar{\boldsymbol{\theta}}^i)$ is also the stationary distribution probability of $(\bar{\boldsymbol{V}}^i, \bar{\boldsymbol{\theta}}^i)$. Furthermore, the distribution probabilities of system states $(\bar{\boldsymbol{V}}, \bar{\boldsymbol{\theta}})$ and the states of measuring devices $\bar{\boldsymbol{U}}$ become mutually independent, i.e.,

$$p_r(s^i) = p_r(\bar{\boldsymbol{V}}^i, \bar{\boldsymbol{\theta}}^i, \bar{\boldsymbol{U}}^i) = q(\bar{\boldsymbol{V}}^i, \bar{\boldsymbol{\theta}}^i) \cdot p_r(\bar{\boldsymbol{U}}^i), \tag{34}$$

where $p_r(\bar{\boldsymbol{U}}^i)$ denotes the stationary distribution of measuring devices at state $\bar{\boldsymbol{U}}^i$. In this case, the number of variables reduces to 2^m in order to compute $p_r(\bar{\boldsymbol{U}}^i)$ from (32). $P(\bar{\boldsymbol{U}}^i | \bar{\boldsymbol{U}}^j)$ can be computed from

$$P(\bar{\boldsymbol{U}}^i | \bar{\boldsymbol{U}}^j) = \textstyle\sum_{(\bar{\boldsymbol{V}}^k, \bar{\boldsymbol{\theta}}^k)} P(\bar{\boldsymbol{U}}^i | \bar{\boldsymbol{V}}^k, \bar{\boldsymbol{\theta}}^k, \bar{\boldsymbol{U}}^j, \hat{\pi}) \cdot q(\bar{\boldsymbol{V}}^k, \bar{\boldsymbol{\theta}}^k), \tag{35}$$

where we skip the derivations due to space limitations.

The computational complexity can be further reduced by sub-sampling the states and approximating $P(\bar{\boldsymbol{U}}^i | \bar{\boldsymbol{U}}^j)$ by

$$P(\bar{\boldsymbol{U}}^i | \bar{\boldsymbol{U}}^j) \approx \frac{\sum_{(\bar{\boldsymbol{V}}^k, \bar{\boldsymbol{\theta}}^k, \bar{\boldsymbol{U}}^j) \in \Psi(s)} P(\bar{\boldsymbol{U}}^i | \bar{\boldsymbol{V}}^k, \bar{\boldsymbol{\theta}}^k, \bar{\boldsymbol{U}}^j, \hat{\pi}) \cdot p_r(\bar{\boldsymbol{V}}^k, \bar{\boldsymbol{\theta}}^k)}{\sum_{(\bar{\boldsymbol{V}}^k, \bar{\boldsymbol{\theta}}^k, \bar{\boldsymbol{U}}^j) \in \Psi(s)} p_r(\bar{\boldsymbol{V}}^k, \bar{\boldsymbol{\theta}}^k)}, \tag{36}$$

where $\Psi(s)$ is the set of sampled states.

After obtaining $p_r(s^i)$, the attack probability $p_b(i)$ of bus i and the attack probability p_{sys} of the whole system can be estimated with the sampled states as follows:

$$p_b(i) \approx \frac{\sum_{s^k \in \Psi(s)} \mathbb{1}_{[i \in \Phi_b(\hat{\pi}(s^k))]} \cdot p_r(s^k)}{\sum_{s^k \in \Psi(s)} p_r(s^k)}, \tag{37}$$

$$p_{sys} \approx \frac{\sum_{s^k \in \Psi(s)} \mathbb{1}_{[\Phi_b(\hat{\pi}(s^k))\text{is not empty}]} \cdot p_r(s^k)}{\sum_{s^k \in \Psi(s)} p_r(s^k)}. \tag{38}$$

V. Simulation

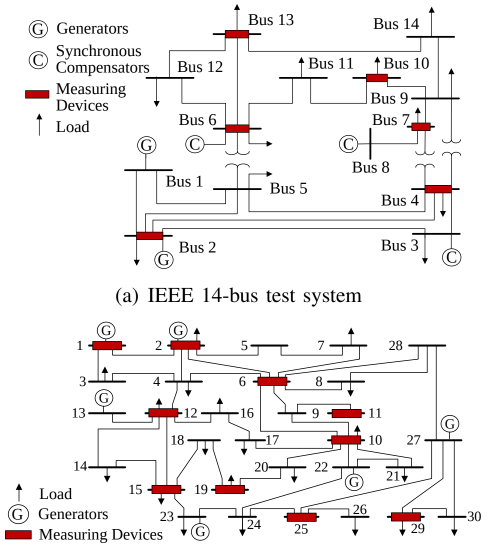
We test our method in the IEEE 14-bus and 30-bus test systems, as shown in Fig. 4. Each measuring device records the voltage phasor of its located bus and the current phasors of incident lines. The system parameters are available in [28].

Given load conditions, the system states are determined from the economic dispatch (ED) (expect for Section V-D), which is implemented with MATPOWER toolbox [29] in MATLAB. The objective of economic power dispatch is to minimize the aggregate fuel cost,

$$\sum_{i=1}^{N} C_i(P_i) = \sum_{i=1}^{N} a_i + b_i P_i + c_i P_i^2, \tag{39}$$

where $C_i(P_i)$ is the fuel cost of generator i to generate P_i active power, and a_i, b_i, c_i are the cost coefficients of generator i. We relax the constraints concerning real power to $P_{ij} \leq 1.2 P_{ij}^M$ in economic dispatch. In the 14-bus system, the capacities of line 1-2 and 1-5 are 100MW, and the capacities of other lines are 50MW. The coefficients of fuel cost and the line capabilities of the 30-bus system are provided in [28].

The common settings except for Section V-C are as follows:



(a) IEEE 14-bus test system

(b) IEEE 30-bus test system

Fig. 4. IEEE test systems

1) Discrete System States. The range of bus voltage magnitude is 0.96 p.u. to 1.06 p.u., and $n_V = 5$. Each bus voltage angle has 9 intervals with a resolution of 1°, thus $n_\theta = 9$. Then there are $5 \times 9 = 45$ ways to inject errors to one target bus.

2) Transition Probability of Measuring Devices. $p_T = 0.5$. The attack detection probability is computed from (16), where $\eta = 5$.

3) Rewards and Costs. $\beta = 2$. $C = 1$ in (16). $g_u = 0.01$ in (22). K_{ij}'s in (19) are all set to be 1.

A. Attacks with knowledge of future system states

The prediction time is 1 hour, during which each load follows the curve in Fig. 5. The system operator conducts state estimation once every five seconds. Thus there are 720 time steps, and $2^6 \cdot 720 = 46080$ (six measuring units) and $2^{10} \cdot 720 = 737280$ (ten measuring units) states in the 14-bus and 30-bus systems, respectively. The discount factor for future rewards $\gamma = 1$.

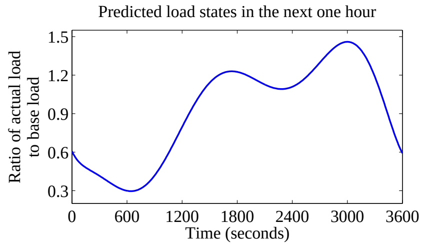


Fig. 5. Predicted load state during one hour

TABLE V
Expected attack probabilities of five most vulnerable buses with varying initial device states in the 14-bus system.

Initial Device States	**Expected Attack Probability**				
on Bus 2,4,6,7,10,13	Bus 10	Bus 2	Bus 8	Bus 9	Bus 7
0, 0, 0, 0, 0, 0	23.15%	11.14%	10.44%	9.90%	7.34%
0, 0, 0, 0, 1, 1	23.25%	11.14%	10.44%	9.90%	7.34%
0, 0, 0, 1, 1, 1	23.24%	11.13%	10.44%	9.90%	7.37%
1, 1, 1, 1, 1, 1	23.25%	11.12%	10.44%	9.88%	7.40%

Table V records the attack probabilities of top five most vulnerable buses in the 14-bus system with different initial states of the measuring devices. ‘0’ and ‘1’ correspond to inaccessible and open to attacks respectively. There is a slight variation in the expected attack probabilities when the initial states vary, because 720 time steps are long enough to mitigate the influence of initial states.

Bus 10 is the most vulnerable one. The reason is twofold. The line connecting bus 9 and bus 10 has a smaller reactance than other lines, then with the same errors injected to the bus voltage phasors, the resulting reward from this line is larger. An adversary only needs to intrude the device on bus 10 to change the bus’s state, hence the attack cost is small.

Similar phenomenon is observed in the 30-bus system. The top five most vulnerable buses are shown in Table VI.

TABLE VI
EXPECTED ATTACK PROBABILITIES OF FIVE MOST VULNERABLE BUSES IN THE FORMULATED FOUR MDP CASES.

MDP Case	**Attack Probabilities of Top Five Most Vulnerable Buses**				
14-bus finite-horizon	Bus 10 23.25%	Bus 2 11.12%	Bus 8 10.44%	Bus 9 9.88%	Bus 7 7.40%
14-bus infinite-horizon	Bus 10 25.00%	Bus 7 18.06%	Bus 9 4.43%	Bus 2 4.00%	Bus 8 2.82%
30-bus finite-horizon	Bus 24 27.29%	Bus 22 24.69%	Bus 15 23.21%	Bus 14 19.20%	Bus 19 17.09%
30-bus infinite-horizon	Bus 19 29.68%	Bus 24 27.72%	Bus 18 18.96%	Bus 22 18.71%	Bus 15 14.46%

B. Attacks with knowledge of state transition probabilities

Each load is assumed to have three states with the ratios of the actual load to the base load being 1/2, 1 and 3/2 respectively. We consider the simple case that at each time instant, every load transits to any state with possibility 1/3. Then the stationary distribution of each state is 1/3. $\gamma = 0.95$.

The basis functions are defined as follows:

1) Basis functions only related to each bus.
For bus i, there are five functions: $\bar{V}_i, \bar{V}_i^2, \bar{\theta}_i, \bar{\theta}_i^2, \bar{V}_i \cdot \bar{\theta}_i$.

2) Basis functions only related to each line.
For line ij, there are two basis functions: $\bar{V}_i\bar{V}_j, \bar{\theta}_i\bar{\theta}_j$.

3) Basis functions related to each measuring devices.
For measuring device k, if it needs to be intruded to manipulate the state of bus i, then there are three basis functions: $\bar{U}_k\bar{V}_i$, $\bar{U}_k\bar{\theta}_i$, $\bar{U}_k\bar{V}_i\bar{\theta}_i$.

4) Constant basis function of 1.

There are 189 basis functions for the 14-bus system and 371 functions for the 30-bus system in total.

We sample 2500 load states uniformly, conduct economic dispatch, and discretize the observed continuous system states. Then 2500 device states are sampled to obtain the state in (15). The state-relevance weight $c(s) = \frac{1}{2500}$ for all sampled states. The penalty weight $\lambda = 0.025$. We use CPLEX to solve (31) and obtain the near-optimal actions of the 2500 states.

Additional 10000 states are further sampled uniformly. With the 12500 samples in total, the approximate state distribution probability of measuring devices is computed following (36). The attack probability of each bus is estimated from (37).

The top five most vulnerable buses in this scenario are shown in Table VI. The time requirements for different problem setups implemented on MATLAB on a desktop with 3.4 GHz Intel Core i7 are summarized as follows:

TABLE VII
RUNNING TIME OF SIMULATIONS

Formulated MDPs	**Running Time of Each Procedure** (second)		
	1	2	3
14-bus Finite-horizon	201.92	35.66	3.55
30-bus Finite-horizon	521.30	3140.43	115.50
14-bus Infinite-horizon	246.93	149.38	0.23
30-bus Infinite-horizon	725.64	2863.85	2.61

Note that we do not optimize the codes to reduce computational time, and the MATLAB environment adds overhead to the computation. In Table VII, Procedure 1 finds all the available attack actions and corresponding rewards for each sampled state. Procedure 2 computes the optimal or near-optimal attack policy. Procedure 3 calculates the attack likelihood of each bus based on the obtained policy.

C. Discussions on the influences of various parameters.

We study the impact of several parameters on the attack probabilities of buses.

1) Parameter C in attack detection probability.

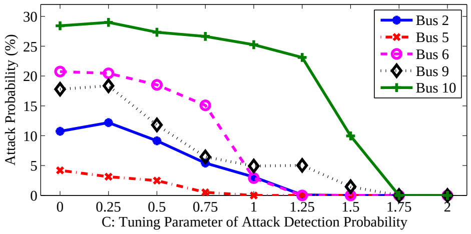


Fig. 6. Attack probabilities of part of buses in the 14-bus system

Fig. 6 shows that the attack probabilities of some buses generally decrease as C increases. The same trend is observed regarding the attack probability of the whole 14-bus system in Fig. 7. That is because when C increases, the detection probability of attacks in (16) increases, and the expected immediate reward in (21) decreases. Bus 10 is always the most vulnerable bus, same as in the finite-horizon MDP.

2) Average cost g_u to intruder one device.

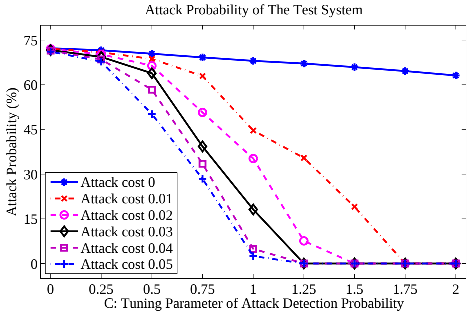


Fig. 7. Influence of attack cost and parameter C on the attack probability of the 14-bus system, $p_T = 0.5$

As shown in Fig. 7, the likelihood of cyber data attacks in the 14-bus system decreases when g_u increases. Same phenomenon is observed in the 30-bus system. Thus, a large intrusion cost contributes positively to preventing the system from cyber data attacks.

3) Device’s state transition probability p_T.

Intuitively, the intruder should be more cautious to launch attacks with a smaller p_T, because devices are more likely to stay inaccessible for a longer time.

Table VIII records the expected attack probabilities of some buses in the 14-bus system with varying p_T. As p_T increases from 0, the expected attack probability of each bus first increases. Then the target buses gradually concentrate on a few buses. The attack probabilities of these buses further increase as p_T increases, while the probabilities of other buses decrease.

4) Maximum number of target buses at each step.

The attack probability of each bus in the 14-bus system is computed with β varying from one to three. Table VIII records the result. One can see the order of buses by the attack probability almost stays the same when β changes. Thus, β does not affect the relative vulnerability of buses much.

TABLE VIII
EXPECTED ATTACK PROBABILITIES OF PART OF BUSES
THE INITIAL STATES OF ALL DEVICES ARE OPEN TO ATTACK, $C = 1$.

β	p_T	**Expected attack probability**				
		Bus 1	Bus 6	Bus 7	Bus 10	Bus 13
1	0	0.16%	0.15%	0.16%	0.15%	0%
	0.5	5.46%	2.76%	7.42%	23.34%	0%
	1	8.03%	0.21%	12.10%	30.47%	0%
2	0	0.16%	0.15%	0.16%	0.15%	0.15%
	0.5	5.45%	3.05%	7.40%	23.19%	3.05%
	1	7.98%	0.39%	19.44%	31.09%	0.39%
3	0	0.16%	0.15%	0.16%	0.15%	0.15%
	0.5	5.16%	3.19%	6.87%	21.87%	3.19%
	1	7.59%	1.19%	10.09%	30.53%	1.19%

5) Discretization of power system states.

We vary n_V and n_θ to study the impact of state discretization on the attack probability of each bus in the 14-bus system.

TABLE IX
EXPECTED ATTACK PROBABILITIES OF FIVE MOST VULNERABLE BUSES WITH VARYING DISCRETIZATION LEVELS OF POWER SYSTEM STATES.

n_V	n_θ	**Attack Probabilities of Five Most Vulnerable Buses** (%)				
		1	2	3	4	5
3	5	10 (23.02)	9 (5.57)	7 (3.80)	8 (0.26)	2 (0)
	7	10 (22.91)	8 (10.53)	7 (7.82)	9 (6.18)	2 (0)
	9	10 (25.08)	7 (7.86)	9 (5.75)	8 (5.41)	2 (1.30)
5	5	10 (22.18)	9 (5.63)	7 (3.81)	8 (0.33)	2 (0)
	7	10 (24.68)	8 (10.75)	7 (7.47)	9 (5.79)	2 (3.30)
	9	10 (23.25)	2 (11.12)	8 (10.44)	9 (9.88)	7 (7.40)

As shown in Table IX, there is only slight variation of attack probabilities when the discretization level changes. The set of most vulnerable buses does not change much.

D. Attacks under different dispatch strategies of the operator

We study the attack likelihood when the operator employs different dispatch strategies with the same set of loads. The intruder does not know the dispatch strategies directly, while it observes the system states resulting from the dispatch strategies.

We employ the environmental/economic dispatch (EED) [30] to obtain variants of dispatch solutions. Besides the fuel cost in (39), EED also considers the pollutant emission. The pollutant emission of the i generator modeled by [30]

$$E_i(P_i) = d_i + e_i P_i + f_i P_i^2, \tag{40}$$

where d_i, e_i, f_i are the emission coefficients of generator i. EED minimizes the weighted sum of fuel cost in (39) and the pollutant emission in (40), which is

$$(1-\delta)\sum_{i=1}^{N} C_i(P_i) + \delta \sum_{i=1}^{N} E_i(P_i),$$

where δ is constant in $[0, 1]$. EED reduces to ED when $\delta = 0$. We employ the coefficients of generator unit 1 to 5 listed in Table I of [30] to measure the emission of generators and compensators in 14-bus system.

We assume that the load state is the same as that in Section V-A, i.e., each load follows the curve of Fig. 5. We solve EED with different δ's to obtain different dispatch solutions. Table X compares some resulting bus voltages at time $t = 1360s$ by choosing $\delta = 0$ and $\delta = 0.5$, respectively.

TABLE X
SYSTEM STATES UNDER DIFFERENT DISPATCH SOLUTIONS.

Bus	**Voltage Magnitude and Angle**	
	Economic Dispatch ($\delta = 0$)	Environmental/Economic Dispatch ($\delta = 0.5$)
1	1.06 p.u., 0°	1.06 p.u., 0°
4	1.01 p.u., -8.17°	1.02 p.u., -7.85°
6	1.06 p.u., -12.27°	1.06 p.u., -11.18°
13	1.04 p.u., -13.15°	1.04 p.u., -12.10°

We assume that the intruder predicts the system states accurately and solves a finite-horizon MDP. The resulting attack likelihood with varying δ is shown in Table XI, where all the measuring units are initially open for attacks. When $\delta \leq 0.15$, the set of most vulnerable buses are almost the same as that in Table V, i.e., when $\delta = 0$. When δ increases, the set of most vulnerable buses changes slightly. Therefore, although different dispatch solutions result in different system states and in turn lead to different optimal attack strategies of the intruder, the set of vulnerable buses do not change much. Therefore, the solution is robust to the intruder's behavior to some degree, and the operator can exploit it to evaluate the system vulnerability.

TABLE XI
EXPECTED ATTACK PROBABILITIES WITH VARYING δ

δ	**Attack Probabilities of Five Most Vulnerable Buses** (%)				
	1	2	3	4	5
0.15	10 (22.38)	7 (11.28)	9 (9.71)	2 (8.93)	8 (6.37)
0.3	10 (23.03)	7 (15.87)	9 (9.15)	6 (6.17)	13 (6.17)
0.7	10 (19.18)	7 (16.45)	9 (12.36)	2 (5.88)	1 (5.84)
1	9 (23.54)	10 (10.37)	1 (4.89)	2 (3.83)	7 (1.04)

E. Deviation from the optimal attack strategy.

In practice, the intruder may not always follow the optimal attack strategy due to either insufficient knowledge about the system state to implement the optimal strategy or the intension to hide its attack pattern. We study the deviation from the optimal strategy with a model that at each time instant, the intruder takes the optimal action with probability p_{opt}. With probability $1 - p_{\text{opt}}$, it selects one available action (including no attack) uniformly at random. When $p_{\text{opt}} = 0$, the attack strategy is completely random. Table XII compares the attack probabilities in the IEEE 30-bus system with finite-horizon attack when p_{opt} changes. All devices are initially accessible.

One can see that as long as p_{opt} is not too small, the set of most vulnerable buses does not change much for the one with the optimal attack strategy.

F. Inaccuracies in the intruder's estimation of system states

So far, the intruder's predictions of the system states are assumed to be accurate. In practice, its predictions may be inaccurate for various reasons. For example, it may not have

TABLE XII
EXPECTED ATTACK PROBABILITIES OF FIVE MOST VULNERABLE BUSES WITH DEVIATIONS FROM THE OPTIMAL ATTACK POLICY.

p_{opt}	**Attack Probabilities of Top Five Most Vulnerable Buses** (%)				
	1	2	3	4	5
0	29 (14.90)	28 (12.53)	24 (11.64)	19 (11.30)	25 (10.25)
0.25	24 (13.84)	19 (13.09)	28 (12.74)	29 (12.63)	15 (11.60)
0.5	24 (17.25)	15 (15.14)	19 (14.61)	22 (13.97)	28 (13.04)
0.75	24 (21.81)	15 (18.98)	22 (18.95)	19 (15.93)	14 (15.27)
1	24 (27.29)	22 (24.69)	15 (23.21)	14 (19.20)	19 (17.09)

access to enough measurements; it may have limited intelligence; or the operator may change its dispatch decision due to the injected data attacks. We next analyze the vulnerability of different components when the intruder's estimation of the system states are not accurate.

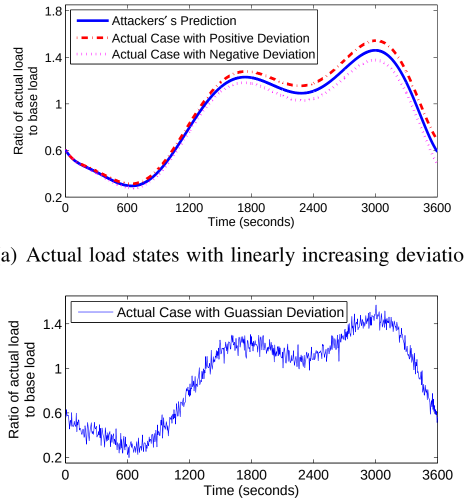
1) *Inaccuracies in the finite-horizon MDP*

In the finite-horizon MDP, we consider the case that an intruder's prediction of the loads deviates from the actual loads. We consider two types of deviation:

(a) the prediction deviates from the actual state with a linearly increasing positive (or negative) drift as time evolves;

(b) at each time instant, the prediction error is a random value drawn from $\mathcal{N}(0, \sigma^2)$.

In the simulation, we set the terminal relative deviation to the base load in type (a) to be 0.1, and $\sigma = 0.05$ in type (b). The corresponding load states are demonstrated in Fig. 8.



(a) Actual load states with linearly increasing deviations

(b) Actual load states with Guassian deviation

Fig. 8. Equivalent influence of the operator's response

TABLE XIII
EXPECTED ATTACK PROBABILITIES OF FIVE MOST VULNERABLE BUSES WITH DEVIATIONS IN THE LOAD ESTIMATION.

Deviation Type	**Attack Probabilities of Top Five Most Vulnerable Buses**				
Positive drift	Bus 10 19.79%	Bus 9 12.18%	Bus 2 10.42%	Bus 7 9.17%	Bus 8 7.22%
Negative drift	Bus 10 22.48%	Bus 7 10.75%	Bus 9 9.94%	Bus 2 8.16%	Bus 8 7.98%
Gaussian error	Bus 10 22.21%	Bus 7 10.84%	Bus 9 9.46%	Bus 2 8.18%	Bus 8 6.26%

Table XIII records the top five most vulnerable buses in the 14-bus system with the above deviation models. All measuring devices are initially open to attacks. The most vulnerable buses are almost the same as the results in Table V when the intruder's state estimation is accurate.

2) *Inaccuracies in the infinite-horizon MDP*

In the infinite-horizon MDP, we assume that the system evolves following a Markov Chain that is different from the intruder's estimated Markov Chain. We first consider the case that the intruder's estimation of the stationary distribution is accurate, but its estimated state transition probabilities are not. In the numerical experiment, every load transits from one state to any of the three states with probability $1/3$. The intruder's estimation, however, is that each load state stays the same with a probability of p_s and transits to any of the other two states with a probability of $(1 - p_s)/2$. Although the estimated stationary distribution is still uniform among the three states, the estimated state transmission probabilities are not accurate (unless $p_s = 1/3$). Table XIV records the set of most vulnerable buses when p_s varies. Compared with Table VI, one can see that the set of top five most vulnerable buses is robust to small variations in p_s, i.e., the inaccuracy in the estimation of the state transition probability.

TABLE XIV
EXPECTED ATTACK PROBABILITIES OF FIVE MOST VULNERABLE BUSES WITH VARYING STATE TRANSITION PROBABILITIES.

p_s	**Attack Probabilities of Top Five Most Vulnerable Buses**				
0	Bus 10 26.66%	Bus 7 16.34%	Bus 13 11.98%	Bus 2 11.95%	Bus 6 8.30%
0.2	Bus 10 27.16%	Bus 7 17.29%	Bus 9 7.42%	Bus 8 3.35%	Bus 2 3.33%
0.4	Bus 10 26.99%	Bus 7 16.56%	Bus 9 7.60%	Bus 8 3.37%	Bus 2 3.36%

We further study the case that the intruder's estimation of the stationary distribution is not accurate either. In the actual case, every load transits from one state to any state with probability $1/3$. The intruder's estimation, however, is that every load transits from any state to state 1, 2 and 3 with probability of p_1, p_2, and p_3, respectively, with $p_1 + p_2 + p_3 = 1$. Then the estimated stationary distribution of load state 1, 2, and 3 is also p_1, p_2, and p_3, respectively. Unless $p_1 = p_2 = p_3 = 1/3$, both the estimated stationary distribution and the estimated transition probabilities are inaccurate. Table XV records part of the results of the vulnerability analysis.

TABLE XV
EXPECTED ATTACK PROBABILITIES OF FIVE MOST VULNERABLE BUSES WITH VARYING STATE STATIONARY DISTRIBUTIONS.

p_1, p_2, and p_3	**Attack Probabilities of Top Five Most Vulnerable Buses**				
0.40, 0.30, 0.30	Bus 10 27.15%	Bus 7 17.29%	Bus 9 7.44%	Bus 8 3.35%	Bus 2 3.33%
0.40, 0.20, 0.40	Bus 10 26.59%	Bus 7 17.58%	Bus 9 8.32%	Bus 8 5.09%	Bus 2 2.86%
0.35, 0.30, 0.35	Bus 10 26.98%	Bus 7 14.52%	Bus 9 8.54%	Bus 2 3.92%	Bus 3 2.76%
0.50, 0.25, 0.25	Bus 13 19.30%	Bus 10 17.84%	Bus 2 14.00%	Bus 6 13.98%	Bus 7 12.57%

When all p_i's are between 0.2 and 0.4, the set of top five most vulnerable buses are almost the same as the results in Table VI, which corresponds to the accurate estimation. Thus, when the estimated distribution does not deviate much from the actual uniform distribution, the results of the vulnerability analysis do not change much. Therefore, even if the intruder has limited information about the system state, the proposed MDP-based approach helps the operator to evaluate the vulnerability of the power system.

Discussions and Summary of Numerical Studies

One important observation from the above study is that the set of most vulnerable components does not change much, when various parameters in the MPD problem change (V-C); or the operator employs different dispatch strategies (V-D); or the intruder's attack strategy deviates from the optimal attack strategy (V-E); or the intruder's estimation about the system states are not accurate (V-F). This property is especially important for the practical application of our method. Some parameters are assumed to be known and accurate in our method, while in practice, the detection probability varies with the specific choice of the detection method; the cost to inject an attack depends on the system's defense mechanism; and the intruder may have limited knowledge about the system state and limited resources to carry out the optimal attacks. Still, the result of our method is robust to these uncertainties to some degree, and the operator can implement our method to study the intruder's attack behavior and evaluate the vulnerability of the system.

VI. Conclusions

This paper for the first time analyzes the likelihood of cyber data attacks to power systems. We model an intruder's attack strategy by a Markov Decision Process (MDP). The attack likelihood is analyzed based on the obtained optimal attack strategy of an intruder.

We conduct experiments on IEEE 14-bus and 30-bus systems and study the impact of several factors on the MDP solution and the attack likelihood. We demonstrate that the operator can also implement out method to study the system vulnerability. Future work includes finding the optimal defense policy for the system operator and updating it in real time.

Acknowledgement

This research is supported in part by the ERC Program of NSF and DoE under the supplement to NSF Award EEC-1041877 and the CURENT Industry Partnership Program, and in part by NSF Grant 1508875, NYSERDA Grants #36653 and #28815.

References

[1] Y. Hao, M. Wang, and J. H. Chow, "Likelihood analysis of cyber data injection attacks to power systems," in *Proc. IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, 2015, pp. 657–661.

[2] A. Abur and A. G. Exposito, *Power system state estimation: theory and implementation*. CRC Press, 2004.

[3] J. Chen and A. Abur, "Placement of PMUs to enable bad data detection in state estimation," *IEEE Trans. Power Syst.*, vol. 21, no. 4, pp. 1608–1615, 2006.

[4] E. Handschin, F. Schweppe, J. Kohlas, and A. Fiechter, "Bad data analysis for power system state estimation," *IEEE Trans. Power App. Syst.*, vol. 94, no. 2, pp. 329–337, 1975.

[5] A. Monticelli and A. Garcia, "Reliable bad data processing for real-time state estimation," *IEEE Trans. Power App. Syst.*, no. 5, pp. 1126–1139, 1983.

[6] H. M. Merrill and F. C. Schweppe, "Bad data suppression in power system static state estimation," *IEEE Trans. Power App. Syst.*, no. 6, pp. 2718–2725, 1971.

[7] W. Xu, M. Wang, J. Cai, and A. Tang, "Sparse error correction from nonlinear measurements with applications in bad data detection for power networks," *IEEE Trans. Signal Process.*, vol. 61, no. 24, pp. 6175–6187, 2013.

[8] O. Kosut, L. Jia, R. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures," in *Proc. IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2010, pp. 220–225.

[9] 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.

[10] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye, "Detecting false data injection attacks on DC state estimation," in *Proc. the First Workshop on Secure Control Systems (SCS)*, 2010, pp. 1–9.

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

[12] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Trans. Autom. Control*, vol. 59, no. 6, pp. 1454–1467, 2014.

[13] 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.

[14] 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.

[15] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," in *Proc. the First Workshop on Secure Control Systems (SCS)*, 2010.

[16] A. Tajer, S. Kar, H. V. Poor, and S. Cui, "Distributed joint cyber attack detection and state recovery in smart grids," in *Proc. IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2011, pp. 202–207.

[17] Y. Shoukry, P. Nuzzo, A. Puggelli, A. L. Sangiovanni-Vincentelli, S. A. Seshia, and P. Tabuada, "Secure state estimation for cyber physical systems under sensor attacks: A satisfiability modulo theory approach," 2015.

[18] 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.

[19] 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 International Conference on Smart Grid Communications (SmartGridComm)*, 2014, pp. 830–835.

[20] C. Y. Ma, D. K. Yau, and N. S. Rao, "Scalable solutions of markov games for smart-grid infrastructure protection," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 47–55, 2013.

[21] M. L. Puterman, *Markov Decision Processes: Discrete Stochastic Dynamic Programming*. John Wiley & Sons, Inc., 1994.

[22] 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.

[23] 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.

[24] D. P. de Farias and B. Van Roy, "On constraint sampling in the linear programming approach to approximate dynamic programming," *Mathematics of operations research*, vol. 29, no. 3, pp. 462–478, 2004.

[25] R. D. Smallwood and E. J. Sondik, "The optimal control of partially observable markov processes over a finite horizon," *Operations Research*, vol. 21, no. 5, pp. 1071–1088, 1973.

[26] Y. Ye, "A new complexity result on solving the markov decision problem," *Mathematics of Operations Research*, vol. 30, no. 3, pp. 733–749, 2005.

[27] M. Petrik and S. Zilberstein, "Constraint relaxation in approximate linear programs," in *Proceedings of the 26th Annual International Conference on Machine Learning*. ACM, 2009, pp. 809–816.

[28] Power System Test Case Archive, [Online], https://www2.ee.washington.edu/research/pstca/.

[29] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, "Matpower: Steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 12–19, 2011.

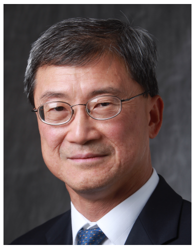
[30] L. Bayón, J. M. Grau, M. M. Ruiz, and P. M. Suárez, "The exact solution of the environmental/economic dispatch problem," *IEEE Trans. Power Syst.*, vol. 27, no. 2, pp. 723–731, 2012.

Yingshuai Hao (S'14) received the B.E. degree from Shandong University, Jinan, China, in 2011 and the M.S. degree in electrical engineering from Shanghai Jiao Tong University, Shanghai, China, in 2014.

He is pursuing the Ph.D. degree in electrical engineering at Rensselaer Polytechnic Institute, Troy, NY. His research interests include cyber security of power systems, and PMU data recovery.

Meng Wang (M'12) received the B.S. and M.S. degrees from Tsinghua University, China, and the Ph.D. degree in 2012 from Cornell University, Ithaca, NY, USA.

She is an Assistant Professor in the department of Electrical, Computer, and Systems Engineering at Rensselaer Polytechnic Institute. Her research interests include high-dimensional data analysis and their applications in power systems monitoring and network inference.



Joe H. Chow (F'92) received the M.S. and Ph.D. degrees from the University of Illinois, Urbana-Champaign, Urbana, IL, USA.

After working in the General Electric power system business in Schenectady, NY, USA, he joined Rensselaer Polytechnic Institute, Troy, NY, USA, in 1987, where he is a Professor of Electrical, Computer, and Systems Engineering. His research interests include power system dynamics and control, FACTS controllers, voltage stability analysis, and synchronized phasor data.