A Cross-Layer Design Approach to Strategic Cyber Defense and Robust Switching Control of Cyber-Physical Wind Energy Systems

Juntao Chen, *Member, IEEE*, and Quanyan Zhu, *Member, IEEE*

***Abstract*— Due to the increasing adoption of smart sensing and Internet of things (IoT) devices, wind energy system (WES) becomes more vulnerable to cyber and physical attacks. Therefore, designing a secure and resilient WES is critical. This paper first proposes a system-of-systems (SoS) framework for the cyber-physical WES. Specifically, on the one hand, we adopt a game-theoretic model to capture the interactions between the WES system defender and the adversary at the cyber layer. The outcome of this cyber defense game is reflected by control-aware Nash equilibria. On the other hand, we devise a cyber-aware robust and resilient switching controller based on a Markov jump linear system model for the physical WES. The performances of the WES cyber and physical layers are interdependent due to their natural couplings. We further investigate the SoS equilibrium of the integrated WES, which considers the system security, robustness, and resilience holistically. Finally, we use case studies to corroborate the developed cross-layer design principles for the cyber-physical WES.**

***Note to Practitioners*—Cybersecurity becomes a critical concern of wind energy system (WES) operators as an increasing amount of IoT devices are adopted for WES's communication, monitoring, and operation support purposes. This cyber-physical integration in WES creates a much broader attack surface because adversaries can compromise the physical WES by attacking its dependent cyberspace. To mitigate the impact of attacks, the operator should not only design intelligent control strategies for WES but also strategically secure the WES's cyber layer. These two goals are naturally coupled together. On the one hand, the WES operates under different compromised conditions depending on the attack actions at the cyber layer. Thus, the control design needs to be adversary-aware by taking the real-time cyber state into account. On the other hand, the adversary's cyberattack strategy is influenced by the induced performance degradation of WES. Hence, the corresponding attack measures and countermeasures, in turn, should be physically control-aware. This paper establishes a holistic mathematical framework to simultaneously address these two challenging objectives. The obtained solution provides guidelines for the WES operator on the optimal security resource investment in defending against cyberattacks and the robust switching control design to mitigate the impacts of attacks further. This methodology creates a defense-in-depth paradigm for the WES operators to maintain the energy system efficiency in the adversarial environment. This cross-layer design approach is also efficient and user-friendly for online implementation with the developed iterative algorithm. The simulated-based case studies in this paper show the effectiveness of the proposed approach. However, a more thorough validation of the method in practice is necessary before its integration with the production standard.**

***Index Terms*— Wind energy system, cyber-physical security, cross-layer design, switching control, interdependence.**

Manuscript received 14 August 2021; revised 8 March 2022; accepted 23 March 2022. Date of publication 12 April 2022; date of current version 6 January 2023. This article was recommended for publication by Editor Q. Zhao upon evaluation of the reviewers' comments. This work was supported in part by the National Science Foundation under Grant ECCS-2138956, Grant ECCS-1847056, Grant CNS-2027884, and Grant BCS-2122060; in part by the Department of Energy-Office of Nuclear Energy (DOE-NE) under Grant 20-19829; and in part by the Army Research Office (ARO) under Grant W911NF-19-1-0041. *(Corresponding author: Juntao Chen.)*

Juntao Chen is with the Department of Computer and Information Sciences, Fordham University, New York City, NY 10023 USA (e-mail: jchen504@fordham.edu).

Quanyan Zhu is with the Department of Electrical and Computer Engineering, Tandon School of Engineering, New York University, Brooklyn, NY 11201 USA (e-mail: qz494@nyu.edu).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TASE.2022.3164860.

Digital Object Identifier 10.1109/TASE.2022.3164860

I. Introduction

WIND energy system (WES) is a critical component of the smart grid to modernize the power grid. One feature of modern WES operation is on its remote control through the support of sensing and communications [1]. Fig. 1 depicts a framework of communication-based remote wind farm control system. Based on the data collected by the local sensors of WES, the supervisory control and data acquisition (SCADA) system first generates the commands and then sends them to the local WES server. This type of WES can be naturally regarded as a cyber-physical system.

The cybersecurity of WES becomes a critical concern due to the integration of information technologies with the WES control systems. Based on the General Electric (GE) report [2], 96% wind farm has at least one machine with a vulnerable operation system. Hence, the attackers can compromise the WES by attacking the SCADA system and turbine controllers, which leads to substantial financial losses, e.g., one-day downtime of a 50 MW wind farm equals to 29k$ loss. Thus, securing the cyberspace of WES is imperative.

One feature of modern cyberattacks is that they are elaborately designed and can be stealthy, e.g., Stuxnet attack [3], such that the traditional firewall approach becomes insufficient to defend against these cyberattacks [2]. Thus, cyber defense in WES should shift from the focus on designing perfect security using firewall methods to best-effort strategic defense. In addition to securing the cyber layer of WES, the WES control system operators need to design robust controllers to further counteract the adversarial impacts due to the cyber-

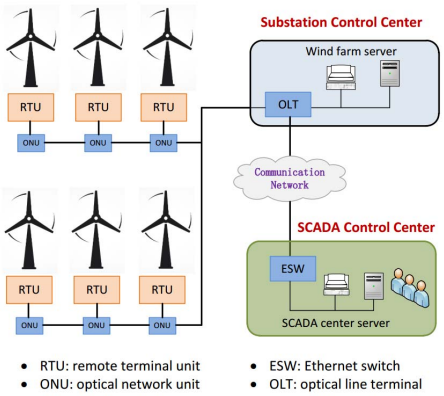


Fig. 1. A communication-based remote wind farm control system includes the SCADA system, communication networks, wind farm local server, and remote terminal units. This type of WES can be seen as a networked control system or cyber-physical system.

physical interdependencies. To this end, our objective is to devise a secure, robust, and resilient cyber-physical WES from a cross-layer perspective that focuses on both cyber layer defense and physical system robust control.

In this work, we establish a non-cooperative game-theoretic framework to capture the behaviors of system defender and cyber attacker. We further develop a Markov jump linear system (MJLS) model for the WES, where the state of MJLS represents the operation condition (e.g., normal or faulty) of the WES. Based on the MJLS model, a robust and resilient switching controller is designed to improve the WES performance. The WES resiliency is quantified by its recovery rates from the post-attack operation mode to the normal operation state. Note that the cyber defender's protection strategy governs the state transition of the WES, further influencing the robust controller design. In addition, the established cyber defense game outcomes have a direct impact on the WES operation efficiency. In sum, the two distinct cyber and physical components of the WES are inherently coupled. Thus, the designed cyber defense strategies need to be control-aware, and in turn, the WES controller design at the physical layer should be cyber-aware. To overcome this challenge, we integrate the cyber-physical layers together through a *system-of-systems* framework. This framework guides a balanced design for achieving WES robustness, security, and resilience.

The main contributions of the paper are presented below.

1) We develop an integrative system-of-systems framework for the holistic modeling of the cyber and physical layers of the smart wind energy systems.
2) We design a robust and resilient stabilizing switching controller based on an MJLS model for the WES through a set of linear matrix inequalities (LMIs). The controller considers the cyber layer of WES and thus incorporates *cyber-aware* characteristic.
3) We provide WES's secure design principles by analyzing a non-cooperative game between the cyber system defender and attacker. The *control-aware* Nash equilibrium solution of the established game is obtained by addressing bilinear programmings (BPs).
4) We formally define the *system-of-systems equilibrium* of the WES and design an algorithm to assess the cyber-physical WES performance under the developed cross-layer design methodology.

A. Related Work

Control of wind renewable energy systems has been studied extensively in literature with various types of intelligent controllers. The WES's resilient design plays a critical role in enhancing the smart grid efficiency [4]–[7]. With the increasing integration of information and communication technologies (ICTs) with the smart grid, cyber-physical security becomes a critical issue in ensuring the efficient power system and critical infrastructure operations [8]–[10]. In [11], an integrated security framework based on a multi-layer intrusion detection system has been designed for power grid automation. A security mechanism based on IEC 61400-25 communication model has been proposed in [12] to protect the large-scale WES from cyberattacks.

Game-theoretic approach has been widely adopted to guide the secure system analysis and design, especially in the cyber-physical systems [13]–[16]. Our cyber-physical cross-layer framework for secure and resilient control design is also related to [17], [18]. However, different from above, we focus on the specific WES security problem and propose an integrative algorithm to achieve the optimal system-of-systems design. The current work extends our preliminary version [19] in multiple aspects. First, we provide detailed WES modeling and state-space representation, facilitating the cyberattack integration with the established framework. Second, we extensively expand the two main technical sections, including the robust and resilient physical system design (Section IV) and the game-theoretic cyber system design (Section V) with sophisticated analysis. Third, we formally introduce the system-of-systems equilibrium in Section VI, and extend Section VII thoroughly to illustrate the WES design principles. Fourth, we provide more illustrations and discussions in each section, e.g., Figs. 1, 4, 5, and 6. Last but not least, we expand and enrich the entire introduction section, discuss more related works, and include a table for notations.

B. Notations

The bold lower case $\mathbf{x}$ is a vector, and the bold upper case $\mathbf{X}$ represents a matrix. The notation $\mathbf{x} = [x_i]_{i\in\mathcal{S}}$ means that vector $\mathbf{x}$ is composed by the elements x_i where i belongs to the set $\mathcal{S}$. The parameters with superscript $'$ and $*$ indicate the transpose and Nash equilibrium, respectively. For clarity, Table I summarizes some critical notations used.

C. Organization of the Paper

The rest of the paper is organized as follows. Section II presents the problem and establishes a system-of-systems framework for the cyber-physical WES. Section III presents WES modeling and cyberattack models. We design a cyber-aware robust and resilient switching controller in Section IV. We establish a secure cyber system design framework and analyze a control-aware cyber defense game in

TABLE I
NOMENCLATURE

ϑ_{op}	Operating point of WES
ϑ_c	Operating condition of WES
ϑ_t	Inclusion of ϑ_{op} and ϑ_c, i.e., $\vartheta_t = [\vartheta_{op}, \vartheta_c]$
$\boldsymbol{\vartheta}_t$	Set of all admissible ϑ_t
$\mathcal{S}$	Set $\mathcal{S} := \{1, 2, ..., S\}$
$\tilde{\mathcal{S}}$	Set $\tilde{\mathcal{S}} := \{0, 1, ..., S-1\}$
γ_{ij}	Transition rate from state i to state j
a_i	Cyber attacker's pure action
d_j	Cyber defender's pure action
$\mathbf{g}$	Cyber attacker's mixed strategy
$\mathbf{f}$	Cyber defender's mixed strategy
P_{ij}	Power generation of WES under action pair $\{a_i, d_j\}$
$C_{a,i}$	Attack cost corresponding to action a_i
$C_{d,j}$	Defense cost corresponding to action d_j

Section V. Section VI proposes an iterative algorithm to compute the solution. Section VII presents case studies to corroborate the obtained results. Finally, Section VIII concludes the paper.

II. Problem Statement and System-of-Systems Framework

A. Problem Statement

Ensuring normal operation of cyber-physical WES under the adversarial environment is a principal task for WES operator given the tremendously increasing cyber threats to the power energy sector. To counteract the cyber attacks effectively, the operator should not only secure the cyber layer of WES directly but also need to further mitigate the adversarial impacts at the physical layer of WES. This work aims to propose a systematic cross-layer approach to achieve this goal by developing both adversary-aware robust control strategy to operate the physical WES and control-aware strategic cyber defense to secure the cyber system of WES.

B. System-of-Systems Framework

The cyber-physical interactions in modern WES require establishing an integrated system framework. We leverage the standardized NIST CPS framework [20] to describe the essential aspects of our proposed model, including its functionality, interactions, trustworthiness, timing, data, and composition.

1) Functionality: The physical layer of WES contains the mechanical parts of WES that govern the generation of renewable energy to meet operational goals. The cyber layer of WES plays an essential role in the remote control of WES with the support of the SCADA system, and it is composed of communication and sensor networks.
2) Interactions: The cyber and physical layers of WES need to work coordinately to achieve a desirable performance. The interactions and influences between these two layers are bidirectional. First, the cyber layer outcome determines the operating condition of the physical WES and hence impacts the control commands. Second, the physical layer performance (i.e., wind output power) impacts the WES operator's policy in safeguarding cyberspace. The bidirectional interactions demonstrate the inherent interdependencies in cyber-physical WES.
3) Trustworthiness: The trustworthiness includes the security and resilience of WES. The security aspect considers the adversarial attacks to the various components of WES through cyber means, including intrusion to the SCADA system, unauthorized access to the critical sensing information (confidentiality), and improper modifications to such information (integrity). The outcome of cyber compromise could be reflected in the physical component, including controller and actuator. Thus, suitable mechanisms are needed to ensure the trustworthiness of the cyber layer of WES. The resilience is concerned with the ability of the physical part of WES to withstand instability due to natural disturbances and unexpected performance degradation due to cyber attacks. We aim to use an effective control design to equip the physical WES with recovery capability.
4) Timing/Control flow: The considered WES is a dynamic system in nature in which we continuously leverage the collected sensor information to develop and implement an effective control policy. The dynamics also exist within the interactions between the cyber and physical layers. Specifically, the timing of events is as follows: 1) the physical operating condition may change due to cyber attacks; 2) the change of physical operating condition is taken into account in the physical controller design which is further reflected in the output wind power; 3) the cyber layer perceives the physical performance change of WES and updates the cyber defense mechanism accordingly; 4) the modified cyber defense yields new operating conditions of physical WES, and the control flow returns to step 1.
5) Data: The data involved consists of two categories. The first category is physical-related, including sensor measurements and output power of WES. This information is used to decide control commands. The second category is cyber-related, including the outcome of the defense-attack analysis at the cyber layer that determines the prospective operating condition of WES. The data mentioned above are either directly available or convenient to derive based on the collected information.
6) Composition: The heterogeneous interactions among WES components require a holistic modeling framework. A convenient composition of these distinct layers can be achieved using a system-of-systems paradigm that integrates complex WES cyber-physical components.

The integrated system-of-systems framework that captures the essential aspects described above is shown in Fig. 2. The natural couplings across layers require us to devise effective WES control and protection schemes from a cross-layer perspective. Therefore, in Section VI, we propose a system-of-systems equilibrium solution concept that facilitates a holistic design of secure, robust, and resilient cyber-physical WES.

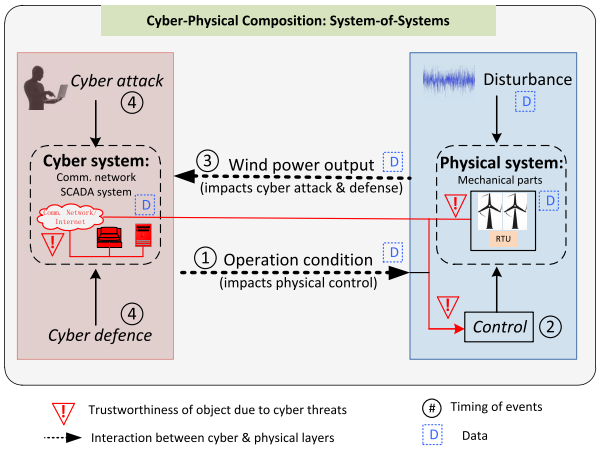


Fig. 2. A system-of-systems framework for modeling cyber-physical WES based on the NIST CPS framework [20]. The cyber layer contains the communication and SCADA components, and the physical layer includes the mechanical parts. The framework also depicts the timing/logical flow of events and data generated/needed for cyber-physical co-design. The attacker acts at the cyber layer, and the consequence could be reflected at the physical controller and actuator.

III. WES Modeling and Cyberattack Models

First, we present the modeling of WES. Then, we introduce three classes of cyberattacks to the cyber-physical WES, which can be integrated with the established WES model.

A. Modeling of WES

To model a WES, we need to consider its aerodynamic system, pitch system, electrical power system, drive train system, and the external wind speed. We briefly describe the WES model here, and more details are referred to [21].

1) Wind Speed: Wind speed $v(t)$ (m/s) is captured by the following two terms [21, Chap. 3.7]

$$v(t) = v_m(t) + \hat{v}(t), \tag{1}$$

where $v_m(t)$ is the mean wind speed; and $\hat{v}(t)$ is the turbulence representing the high-frequency variable component of the wind. The turbulence part $\hat{v}(t)$ is often modeled by the Gaussian white noise.

2) Aerodynamic System: The aerodynamic power P_r (W) captured by the rotor is [22]

$$P_r(t) = \frac{\pi \rho R^2}{2} C_p(\lambda, \beta) v(t)^3, \tag{2}$$

where ρ is the air density (kg/m^3); R is the radius of wind turbine rotor (m); and C_p is the power coefficient which depends on the pitch angle β and the tip speed ratio λ. Here, $\lambda = \omega_r R/v$, where ω_r is the rotor speed (rad/s). The rotor torque $T_r(t)$ (N·m) is given by [22]

$$T_r(t) = \frac{P_r}{\omega_r} = \frac{\pi \rho R^3}{2} C_q(\lambda, \beta) v(t)^2, \tag{3}$$

where $C_q = \frac{C_p}{\lambda}$ is the torque coefficient.

3) Pitch System: A second-order dynamical system is used to model the hydraulic pitch actuator system, given by [23]

$$\ddot{\beta}(t) = -2\zeta\omega_n \dot{\beta}(t) - \omega_n^2 \beta(t) + \omega_n^2 \beta_d, \tag{4}$$

where ω_n is the natural frequency (rad/s), ζ is the damping ratio, and β_d is the commanded pitch angle. Additionally, the values of $\beta(t)$ and its slew rate $\dot{\beta}(t)$ both are bounded.

4) Drive Train System: The drive train includes a gear box, which gears up the rotation speed of rotor to a higher generator speed, and the purpose is to transfer torque from the rotor side to the generator side. Its dynamics are described as follows [21, Chap. 3.2]:

$$J_r \dot{\omega}_r = T_r - K_{dt}\theta_\Delta - (B_{dt} + B_r)\omega_r + \frac{B_{dt}}{N_g}\omega_g, \tag{5}$$

$$J_g \dot{\omega}_g = \frac{B_{dt}}{N_g}\omega_r + \frac{K_{dt}}{N_g}\theta_\Delta - \left(\frac{B_{dt}}{N_g^2} + B_g\right)\omega_g - T_g, \tag{6}$$

$$\dot{\theta}_\Delta = \omega_r - \frac{1}{N_g}\omega_g, \tag{7}$$

where J_r is the rotor inertia (kg·m^2); J_g is the generator inertia (kg·m^2); T_g is the generator torque (N·m); ω_g is the generator speed (rad/s); B_r is the rotor friction coefficient (N·m·s/rad); B_g is the generator friction coefficient (N·m·s/rad); K_{dt} is the torsion stiffness (N·m·s/rad); B_{dt} is the torsion damping coefficient (N·m·s/rad); θ_Δ is the torsion angle.

5) Electrical System: The generator and converter belong to the electrical part of the system, and their dynamics are much faster than the mechanical dynamics. For simplicity, it can be modeled as a first-order system [21, Chap. 3.4]

$$\dot{T}_g = -\frac{1}{\tau_g} T_g + \frac{1}{\tau_g} T_{gd}, \tag{8}$$

where τ_g is the time constant, and T_{gd} is the commanded generator torque (N·m).

B. WES System Representation

For controller design, a linearized model of the system is convenient. The major nonlinear part in the system is the aerodynamic torque. We linearize (3) around the operating point $\vartheta_{op} := (\bar{v}, \bar{\beta}, \bar{\omega}_r)$, and arrive at [21, Chap. 3.6]

$$\hat{T}_r(\vartheta_{op}) = K_r(\vartheta_{op})\hat{\omega}_r + K_v(\vartheta_{op})\hat{v} + K_\beta(\vartheta_{op})\hat{\beta}, \tag{9}$$

where

$$K_r(\vartheta_{op}) = \left.\frac{\partial T_r}{\partial \omega_r}\right|_{\vartheta_{op}} = \frac{\rho\pi R^2 v^2}{2\omega_r}\Big(R\frac{\partial C_p(\lambda,\beta)}{\partial \lambda} - C_p(\lambda,\beta)\frac{v}{\omega_r}\Big),$$

$$K_v(\vartheta_{op}) = \left.\frac{\partial T_r}{\partial v}\right|_{\vartheta_{op}} = \frac{\rho\pi R^2 v}{2}\Big(3C_p(\lambda,\beta)\frac{v}{\omega_r} - R\frac{\partial C_p(\lambda,\beta)}{\partial \lambda}\Big),$$

$$K_\beta(\vartheta_{op}) = \left.\frac{\partial T_r}{\partial \beta}\right|_{\vartheta_{op}} = \frac{\rho\pi R^2 v^3}{2\omega_r}\frac{\partial C_p(\lambda,\beta)}{\partial \beta},$$

and $\hat{T}_r, \hat{\upsilon}, \hat{\beta}$ and $\hat{\omega}_r$ are the deviations from the operating point. Note that the operating point of the WES is time-varying due to the stochastic wind. The linearized WES model is given by

$$\begin{aligned} \dot{x}(t) &= A(\vartheta_t)x(t) + B(\vartheta_t)u(t) + E(\vartheta_t)\hat{\upsilon}(t), \\ y(t) &= C(\vartheta_t)x(t), \end{aligned} \tag{10}$$

where $A(\vartheta_t)$, $B(\vartheta_t)$, $E(\vartheta_t)$ and $C(\vartheta_t)$ are system matrices with appropriate dimensions; $x(t)$ is the state vector; $u(t)$ is the control input; $\hat{\upsilon}(t)$ is the exogenous perturbation; and $y(t)$ is the measured output. In addition, $\vartheta_t := [\vartheta_{op}, \vartheta_c] \in \boldsymbol{\vartheta}_t$ includes the operating point ϑ_{op} and operating condition ϑ_c of the wind turbine, where $\boldsymbol{\vartheta}_t$ is a set of all admissible ϑ_t. Note that the operating condition ϑ_c of WES is determined by the cyber layer of the system-of-systems framework in Fig. 2. For example, under the normal operating condition, the state-space model of WES can be captured by

$$\begin{aligned} \dot{x}(t) = &\begin{bmatrix} -\frac{1}{\tau g} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & -\omega_n^2 & -2\zeta\omega_n & 0 & 0 & 0 \\ 0 & a_{42} & 0 & a_{44} & \frac{B_{dt}}{N_g J_r} & -\frac{K_{dt}}{J_r} \\ -\frac{1}{J_g} & 0 & 0 & \frac{B_{dt}}{N_g J_g} & a_{55} & \frac{K_{dt}}{N_g J_g} \\ 0 & 0 & 0 & 1 & -\frac{1}{N_g} & 0 \end{bmatrix} \\ &\times x(t) + \begin{bmatrix} \frac{1}{\tau g} & 0 \\ 0 & 0 \\ 0 & \omega_n^2 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix} u(t) + \begin{bmatrix} 0 \\ 0 \\ 0 \\ \frac{K_v(\bar{V}, \bar{\beta}, \bar{\omega}_r)}{J_r} \\ 0 \\ 0 \end{bmatrix} \hat{\upsilon}(t), \\ y(t) = &\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} x(t), \end{aligned} \tag{11}$$

where $x = [\hat{T}_g, \hat{\beta}, \hat{\dot{\beta}}, \hat{\omega}_r, \hat{\omega}_g, \hat{\theta}_\Delta]^T$, $u = [\hat{T}_{gd}, \hat{\beta}_d]^T$, $a_{42} = K_\beta(\vartheta_{op})/J_r$, $a_{44} = -(B_{dt} + B_r)/J_r + K_r(\vartheta_{op})/J_r$, $a_{55} = -(B_{dt} + N_g B_g)/(N_g^2 J_g)$ and $y = [\hat{T}_g, \hat{\beta}, \hat{\omega}_r, \hat{\omega}_g]^T$.

When the cyber layer shown in Fig. 2 is not secure, the WES model (10) needs modification to incorporate the impacts of cyberattacks on the physical layer, which is detailed in the following section.

C. Adversarial Modeling

In the following, we present three classes of cyberattacks to the WES.

1) Sensor Attacks: One of the major types of malicious attacks in cyber-physical systems is the sensor attack [24], [25]. For instance, the adversary can compromise the sensing information in a strategic manner during the transmission through a man-in-the-middle attack. This type of attack can be captured using a sensor gain proportional modification model. In WES, we consider the following two sensor attacks: (i) pitch angle measurement sensor attack and (ii) generator speed measurement sensor attack. The sensor attack (i) yields modifications of the modeling of pitch system as well as the pitch angle measurement. Equivalently, the corresponding elements in matrices $B(\vartheta_t)$ and $C(\vartheta_t)$ are altered. To capture sensor attack (ii), we modify the matrices $A(\vartheta_t)$ and $C(\vartheta_t)$ in a similar way.

2) Actuator Attack: The second type of cyberattack targets the WES actuator. The adversary intrudes into the internal WES system and compromises the power converter controller. The mechanism of this actuator attack is similar to the Stuxnet [3], where the physical control system is corrupted. This actuator attack leads to an error on the generators' output torque, which is further reflected by the adjustment of $A(\vartheta_t)$ and $B(\vartheta_t)$.

3) Controller Attack: As shown in Fig. 1, WES is based on the remote control in which the SCADA system decides the control policies and then sends them to the local controller of WES via communications. The integration of ICTs makes the cyber-physical WES vulnerable to attacks [9]. For example, the attackers can launch an attack by compromising the control signal stealthily by invading the SCADA system. This controller attack yields a modification of $B(\vartheta_t)$ in (10).

It is assumed that the cyber threats persist over the entire WES operation. The adversary can exploit the cyber vulnerabilities and launch the attack to influence the WES's operating condition and hence the output power at the physical layer. The attacker's strategy (i.e., targeting sensor, actuator, or controller) may change over time, aiming to yield a successful attack maximally. The defender considers this malicious behavior and develops the strategic defense accordingly, maintaining the WES's normal operation with high-level confidence.

The considered cyberattacks can be integrated with the established WES model (10) by modifying the associated system matrices. Also, multiple attacks may happen simultaneously, and their impacts on the system modeling should be considered jointly in the corresponding matrices. Note that under different cyberattacks, the physical WES operates under various conditions. This adversarial attack needs to be incorporated into the control design.

The cyberattacks considered in this work focus on the mechanical part of WES. It is also possible that the adversary targets the electrical system, e.g., power converters and generators of WES, by compromising their control and state signals transmitting over communication networks. Knowing that the electrical system dynamics are much faster than the mechanical counterpart, the attacks to the former component can propagate more quickly revealed at the compromised generator torque. It hence requires defensive schemes, including attack detection and mitigation, to respond to the adversaries more rapidly. Developing effective strategies to jointly counteract cyberattacks to WES's electrical and mechanical parts is essential, and we aim to address it in future work.

IV. Robust and Resilient Cyber-Aware Switching Control Design

The operating condition of WES is related to the considered cyberattacks. In this section, we design a switching controller for WES based on its Markov jump linear system (MJLS) representation aiming to improve the WES performance.

A. MJLS Model of WES

The cyber-physical WES operates at various operating conditions captured by $\vartheta_c \in \boldsymbol{\vartheta}_c := \{\vartheta_n, \vartheta_{pa}, \vartheta_{gs}, \vartheta_{ac}, \vartheta_{ss}\}$, where $\vartheta_n, \vartheta_{pa}, \vartheta_{gs}, \vartheta_{ac}$ and ϑ_{ss} denote the normal, pitch angle sensor attack, speed sensor attack, actuator attack and controller attack, respectively. Note that the dynamic operating point ϑ_{op} of WES is determined by the wind speed which admits a value in an appropriate subset of $\mathbb{R}^+$. One method for WES controller design is using gain-scheduling by choosing a set of operating points. In this way, the complexity of the WES controller depends on the cardinality of the selected operating point set. In this paper, we specifically focus on the rated output power range of WES, which leads to a fixed assumed ϑ_{op}. This focused scenario indicates that the variance of wind speed is limited, and the references $\bar{\beta}$ and $\bar{\omega}_r$ can be determined before the control design. Therefore, the parameters $K_r(\vartheta_{op})$, $K_v(\vartheta_{op})$ and $K_\beta(\vartheta_{op})$ in (9) can be seen as constants. However, the modeling can be extended to time-varying operating point scenarios depending on the number of chosen operating points during gain-scheduling. Note that though the reference of operating point can be seen as a prior, the WES operating condition is time-varying and depends on the real-time cyber state, which introduces challenges to the control design.

The model presented in (10) can be regarded as an MJLS for WES under different operating conditions. We denote by $\{\vartheta_t, t \geq 0\}$ a right-continuous Markov chain on the complete probability space $(\Omega, \mathcal{F}, \{\mathcal{F}_t\}_{t\geq 0}, \mathbb{P})$, where Ω is the sample space; $\mathcal{F}$ is a σ-algebra of subsets of Ω; $\mathcal{F}_t$ is a filtration; and $\mathbb{P}$ is a probability measure on the measurable space $(\Omega, \mathcal{F})$. ϑ_t takes value in $\mathcal{S} = \{1, 2, \ldots, S\}$ with generator $\Gamma = \{\gamma_{ij}\}_{i,j\in\mathcal{S}}$ given by

$$\mathbb{P}\{\vartheta_{t+\Delta} = j \mid \vartheta_t = i\} = \begin{cases} \gamma_{ij}\Delta + o(\Delta), & \text{if } i \neq j, \\ 1 + \gamma_{ii}\Delta + o(\Delta), & \text{if } i = j, \end{cases} \tag{12}$$

where $\Delta > 0$; $\gamma_{ij} \geq 0$ is the transition rate from state i to state j when $i \neq j$, and $\gamma_{ii} = -\sum_{j=1, j\neq i}^{S} \gamma_{ij}$. For clarity, Fig. 3 depicts the state transition of the WES. Specifically, the states from 1 to 5 representing the WES operates under the normal, pitch angle sensor attack, speed sensor attack, actuator attack, and controller attack scenarios, respectively. For the considered model, there are $S = 5$ operating conditions in total. The transition rates γ_{ij}, $i = 1, \forall j \neq 1 \in \mathcal{S}$, correspond to the attacker's behavior that leads to a failure of WES.

B. Cyber-Aware Robust Switching Controller Design

Our next goal is to design a robust switching controller for the WES based on the established MJLS model. When $\vartheta_t = i \in \mathcal{S}$, we denote $A(\vartheta_t) := A_i$ for convenience, and similar for $B(\vartheta_t)$, $C(\vartheta_t)$ and $E(\vartheta_t)$. Based on [26], the designed dynamic output feedback controller takes the following form:

$$\begin{aligned} \dot{x}_F(t) &= A_F(\vartheta_t)x_F(t) + B_F(\vartheta_t)y(t), \\ u(t) &= C_F(\vartheta_t)x_F(t), \end{aligned} \tag{13}$$

where $A_F(i) = A_{Fi}$, $B_F(i) = B_{Fi}$ and $C_F(i) = C_{Fi}$ are system matrices, $\forall i \in \mathcal{S}$; and $x_F(t)$ represents the state of the designed controller. Under this feedback control, the WES switches between the designed robust controllers agilely based on the measured ϑ_t. Furthermore, the closed-loop system needs to have a level κ of H_∞ noise attenuation, i.e.,

$$\int_0^\infty \mathbb{E}(|z(t)|^2)dt < \kappa^2 \int_0^\infty \mathbb{E}(|\hat{v}(t)|^2)dt, \tag{14}$$

where κ is a prescribed positive constant; $\mathbb{E}(\cdot)$ denotes the expectation operator; $|\cdot|$ is the standard Euclidean norm; $\hat{v}(t)$ is the exogenous perturbation in (10); and $z(t)$ is defined as $z(t) := Q(\vartheta_t)x(t) + R(\vartheta_t)u(t)$ with $Q(\cdot) \succeq 0$ and $R(\cdot) \succeq 0$. For $\vartheta_t = i \in \mathcal{S}$, we denote $Q(\vartheta_t) = Q_i$ and $R(\vartheta_t) = R_i$. Then, for $\forall i \in \mathcal{S}$, the dynamic controller (13) admits the following forms [26]:

$$\begin{aligned} A_{Fi} &= (Y_i^{-1} - X_i)^{-1} M_i Y_i^{-1}, \\ B_{Fi} &= (Y_i^{-1} - X_i)^{-1} L_i, \\ C_{Fi} &= F_i Y_i^{-1}, \end{aligned} \tag{15}$$

where $M_i = -A_i' - X_i A_i Y_i - X_i B_i F_i - L_i C_i Y_i - Q_i'(Q_i Y_i + R_i F_i) - \kappa^{-2} X_i E_i E_i' - \sum_{j=1}^{S} \gamma_{ij} Y_j^{-1} Y_i$. X_i, Y_i, L_i and F_i are the solutions to the following linear matrix inequalities (LMIs):

$$\begin{bmatrix} T_1 & Y_i'Q_i' + F_i'R_i' & \mathcal{R}_i(Y) \\ Q_iY_i + R_iF_i & -I & 0 \\ \mathcal{R}_i'(Y) & 0 & \mathcal{D}_i(Y) \end{bmatrix} \prec 0,$$
$$\begin{bmatrix} T_2 & X_iE_i \\ E_i'X_i & -\kappa^2 I \end{bmatrix} \prec 0, \quad \begin{bmatrix} Y_i & I \\ I & X_i \end{bmatrix} \succ 0, \tag{16}$$

where $T_1 := A_iY_i + Y_iA_i' + B_iF_i + F_i'B_i' + \gamma_{ii}Y_i + \kappa^{-2}E_iE_i'$, $T_2 := A_i'X_i + X_iA_i + L_iC_i + C_i'L_i' + Q_i'Q_i + \sum_{j=1}^{S}\gamma_{ij}X_j$, $\mathcal{R}_i(Y) := [\sqrt{\gamma_{1i}}Y_i, \ldots, \sqrt{\gamma_{(i-1)i}}Y_i, \sqrt{\gamma_{(i+1)i}}Y_i, \ldots, \sqrt{\gamma_{Si}}Y_i]$, and $\mathcal{D}_i(Y) := -\text{diag}(Y_1, \ldots, Y_{i-1}, Y_{i+1}, \ldots, Y_S)$. Note that the feedback controller (13) depends on the system matrices as well as the measurement $y(t)$. The specific values of A_{Fi}, B_{Fi}, and C_{Fi} in (13) are obtained by solving LMIs in (16). The solutions to (16) may not be unique, as these LMIs merely serve as convex constraints on the decision variables. Any feasible solution to (16) is able to achieve our control design goal, i.e., the closed-loop system has a level κ of H_∞ noise attenuation. One possible approach to obtain

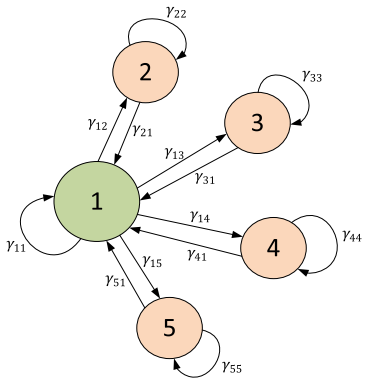


Fig. 3. State transition representation of the WES. State 1 is the normal operation, and states 2 to 5 represent the system operates under the pitch angle sensor attack (ϑ_{pa}), speed sensor attack (ϑ_{gs}), actuator attack (ϑ_{ac}) and controller attack (ϑ_{ss}), respectively. Also, $\{\gamma_{12}, \gamma_{13},\ldots,\gamma_{15}\}$ and $\{\gamma_{21}, \gamma_{31},\ldots,\gamma_{51}\}$ capture the security and resilience of the WES, respectively.

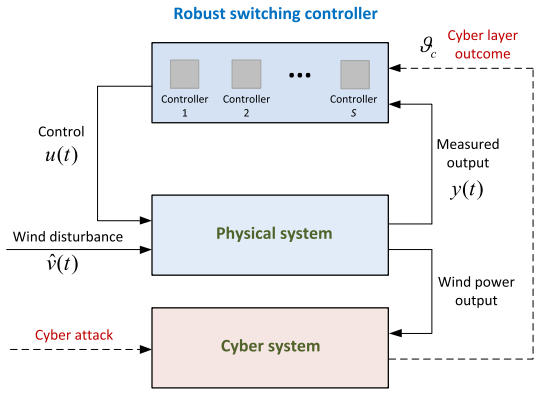


Fig. 4. The structure of the robust switching controller for WES. Based on the outcome of the cyber layer (which determines the operating condition ϑ_c), the WES can switch between different designed robust controllers swiftly.

a unique controller is to construct an objective function in the optimal control framework. The extension to this optimal design scenario is of interest for future work.

The MJLS (10) coupled with the dynamic controller (13) with parameters (15) is mean-square stable [26], and this ensures the stability of the WES under adversary environment. This type of controller (13) has also been shown effective in other industrial applications, including vehicle coordination [27], solar thermal receiver operation and robotic manipulation (Chap. 8, [28]). Note that the controller (13) is not the only choice that can achieve our goal. There are other forms of controller that we can leverage, such as observer-based control, sliding mode control, passivity-based feedback control. For the purpose of this work, the controller in (13) is sufficient to achieve the cyber awareness of WES, where the parameters of the controller can be computed efficiently. Another practical factor that can be considered in the control applications is the delays presented in the system dynamics (e.g., state and output measurement processes). To capture this aspect, instead of using (13), more sophisticated control design is needed for our WES application scenario. For example, one can leverage the dynamic output feedback-based robust switching control designed under time-varying delay with guaranteed exponential stability in [29] to achieve the goal. If the control cost is further considered, one can resort to the robust switching control developed in [30], [31] where both delays and cost metric are included in the problem. Extension in this direction is left as subsequent work.

An illustration of the designed robust switching controller for WES is shown in Fig. 4. One advantage of the designed control over non-switching control (adversary-unaware) is that it explicitly takes into account the real-time cyber state of WES and thus can respond to the adversary with agility to mitigate its imposed impacts on the WES. Specifically, the control operation scheme will switch between the designed controllers based on the cyber state ϑ_t quickly to counteract the adversarial manipulation of the WES.

C. WES Resilience

In the MJLS model, the transition rates γ_{ji}, $i = 1$, $j \neq i \in \mathcal{S}$, represent the resilient ability of WES. The WES exhibiting a faster restoration from the failure state to the normal mode is more resilient to cyberattacks, and a larger γ_{ji} reflects this fact. Note that removing the cyberattacks is costly for the WES operator. Therefore, the operator needs to take into account the tradeoff between the system recovery and the secure WES design costs. Recall that (15) is related to the system restoration transition rates, and thus the designed switching controller captures the resilience of the WES. For clarity, the transition rates γ_{ji}, $i = 1$, are considered as fixed in the current work. The extension to incorporate unfixed restoration cost where γ_{ji}, $i = 1$ are decision variables is nontrivial and requires another layer of optimization.

V. Non-Cooperative Game-Theoretic Control-Aware Cyber System Design

The cyber layer of WES directly influences its physical components as the cyber layer security governs the physical system state transition rates. As perfect cybersecurity is cost-prohibitive, the system operator needs to allocate his defensive resources optimally. To this end, it requires the operator to understand the cyber attacker's strategic behavior and develop the defensive mechanism accordingly. To achieve this goal, we establish a non-cooperative game-theoretic control-aware framework that captures the strategic interactions between the defender and attacker at the cyber layer of WES. This framework facilitates the prediction of security risks of the cyber system under strategic attacks.

A. Control-Aware Cyber Defense Game

We denote this cyber game as $\mathbf{G}_c$. The first step is to identify the action sets for both the attacker and the defender. Specifically, the modeled cyberattacks in Section III-C are sequentially denoted as a_1, a_2, a_3, and a_4, respectively. The SCADA system can monitor the wind farm operation and detect cyber intrusions. According to the attack types, the defensive strategies can be categorized into sensor, actuator, and controller defense. Similarly, we denote the defender's action with respect to the corresponding attack by d_1, d_2, d_3 and d_4, respectively. In addition, both attacker and defender can be inactive which are denoted as a_0 and d_0. Therefore, the attacker's action a belongs to the set $\mathcal{A} := \{a_0, a_1, a_2, a_3, a_4\}$, and the defender's action d is chosen from $\mathcal{D} := \{d_0, d_1, d_2, d_3, d_4\}$. The mixed strategies of attacker and defender are $\mathbf{g} = [g_i]_{i=0}^{S-1} \in \mathcal{G}$ and $\mathbf{f} = [f_i]_{i=0}^{S-1} \in \mathcal{F}$, respectively, where g_i and f_i are the probabilities of choosing $a_i \in \mathcal{A}$ and $d_i \in \mathcal{D}$, respectively. The admissible strategies of two players are denoted as follows:

$$\mathcal{G} := \{\mathbf{g} \in [0,1]^S : \sum_{i=0}^{S-1} g_i = 1\},$$
$$\mathcal{F} := \{\mathbf{f} \in [0,1]^S : \sum_{j=0}^{S-1} f_j = 1\}. \tag{17}$$

The next step is to define the payoff functions of both players in the game $\mathbf{G}_c$. Under a pure strategy profile $\{a_i, d_j\}$, the WES's average output power in a fixed time horizon is

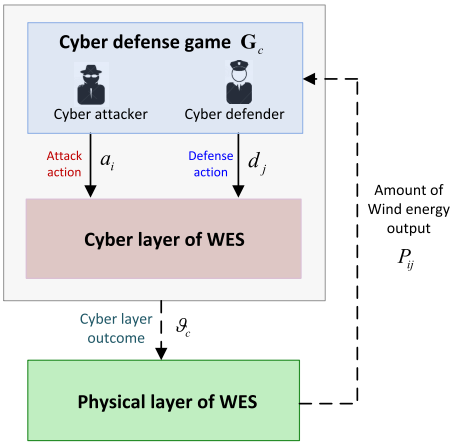


Fig. 5. A non-cooperative game-theoretic framework that models the cybersecurity of WES. Both the attacker and the defender make strategic decisions to optimize their objectives, and their strategies are dependent on the wind power output. Due to the inner coupling, the physical system's performance is influenced by the security game outcome at the cyber layer.

P_{ij}, $i, j \in \tilde{\mathcal{S}} := \{0, \ldots, S-1\}$. The costs of actions a_i and d_j for the attacker and defender are $C_{a,i}$ and $C_{d,j}$, respectively. Specifically, we have the null-strategy costs: $C_{a,0} = 0$ and $C_{d,0} = 0$. With strategy pair $\{a_i, d_j\}$, the defender's utility is

$$U_{ij} = \alpha P_{ij} - C_{d,j}, \tag{18}$$

and the attacker's cost is

$$C_{ij} = \alpha P_{ij} + C_{a,i}, \tag{19}$$

for $i, j \in \tilde{\mathcal{S}}$, where $\alpha > 0$ is a weighting constant. Note that the defender is a maximizer and the attacker is a minimizer in the established nonzero-sum cyber game. The strategy outcome of the game determines the operation state transition rates γ_{ij}, $i = 1, \forall j \neq i \in \mathcal{S}$, of the WES in (12) which affects the performance of the wind energy physical system through (16). Fig. 5 illustrates the game-theoretic framework that captures the WES's cybersecurity, which also shows the explicit interdependencies between the cyber and physical layers of WES.

For a given cyber strategy pair $\{\mathbf{g}, \mathbf{f}\}$, the transition rate γ_{1i} takes the form $\gamma_{1i} = \sum_{j \neq i-1, j \in \tilde{\mathcal{S}}} \eta f_j g_{i-1}$, for $i \neq 1 \in \mathcal{S}$, where η is a relatively small positive weighting constant transforming the probability to a rate measure such that γ_{1i} models realistic cyberattack frequencies. Further, $\gamma_{11} = -\sum_{i \neq 1 \in \mathcal{S}} \gamma_{1i}$. Note that γ_{1i} indicates that the attack a_{i-1} is successful only if the defender's action is not d_{i-1}. The expected attack and defense costs of players are given by $C_a = \sum_{i \in \tilde{\mathcal{S}}} C_{a,i} g_i$ and $C_d = \sum_{j \in \tilde{\mathcal{S}}} C_{d,j} f_j$, respectively. The defender and attacker determine their strategies by considering the tradeoff between the achieved security and incurred cost.

B. Control-Aware Nash Equilibrium

A natural solution concept to characterize the strategies of two players with competing goals is *Nash equilibrium* (NE) composed by $\{\mathbf{g}^*, \mathbf{f}^*\}$. Denote $\mathbf{U} = [U_{ij}]_{\forall i,j \in \tilde{\mathcal{S}}}$ and $\mathbf{C} = [C_{ij}]_{\forall i,j \in \tilde{\mathcal{S}}}$. Then, the definition of NE in mixed strategies of the cyber game is as follows.

Definition 1 (Control-Aware NE of Cyber Game $\mathbf{G}_c$): A strategy pair $\{\mathbf{g}^* \in \mathcal{G}, \ \mathbf{f}^* \in \mathcal{F}\}$ constitutes a non-cooperative NE of the cyber defense game $\mathbf{G}_c$ in mixed strategies if

$$\mathbf{f}' \mathbf{U} \mathbf{g}^* \leq \mathbf{f}^{*\prime} \mathbf{U} \mathbf{g}^*, \quad \text{and } \mathbf{g}^{*\prime} \mathbf{C} \mathbf{f}^* \leq \mathbf{g}' \mathbf{C} \mathbf{f}^*, \tag{20}$$

for $\forall \mathbf{f} \in \mathcal{F}$, and $\forall \mathbf{g} \in \mathcal{G}$.

Under the NE, the expected payoffs are $\bar{U} := \mathbf{f}^{*\prime} \mathbf{U} \mathbf{g}^*$ and $\bar{C} := \mathbf{g}^{*\prime} \mathbf{C} \mathbf{f}^*$ for the defender and attacker, respectively. The existence of mixed strategy NE of the cyber game $\mathbf{G}_c$ is ensured by Nash's Theorem [32]. In addition, the mixed strategy NE can be obtained through solving a bilinear programming (BP).

Remark: The control-aware NE provides the system operator a mechanism to strategically defend the cyber system of WES. One prominent feature of such cyber strategy is its consideration of induced impacts on the physical WES performance in the design loop, which accounts for the cyber-physical interdependencies. Another advantage of the proposed defense scheme is that it fully anticipates the behavior of the cyber attacker and responds to the adversary in a strategic manner compared with cyber defense methods without risk prediction.

VI. Interdependent WES Analysis and Design

Designing cyber and physical layers of cyber-physical systems is generally separate. However, as shown in Sections IV and V, the design of an efficient WES requires a holistic method by integrating the cyber system design and the physical controller design. Therefore, the switching control and the defensive strategy of cyber-physical WES are interdependent. In this section, we first define a system-of-systems equilibrium solution concept for the integrated system and then propose an iterative algorithm to obtain this equilibrium which guides the holistic design of cyber-physical WES.

A. System-of-Systems Equilibrium

The NE security strategies of game $\mathbf{G}_c$ in Section V is computed by BP, and the LMI facilitates the switching controller design in Section IV. The resulting controller of LMI impacts the average WES's output power P_{ij}, $\forall i, j \in \tilde{\mathcal{S}}$, over $t \in [0, T]$. Thus, the LMI's outcome provides an input to the BP to form the game $\mathbf{G}_c$ at the cyber layer. Note that the NE of $\mathbf{G}_c$ determines the state transition rates γ_{ij}, $\forall i, j \in \mathcal{S}$, and consequently impacts the LMI in (16). In sum, we can predict the outcome of the coupled cyber and physical layers of WES by finding a *consistent solution* that satisfies BP and LMI at the same time. We propose the following concept of *system-of-systems equilibrium* to assess the design of the interdependent cyber-physical WES.

Definition 2 (System-of-Systems Equilibrium): The system-of-systems equilibrium in the interdependent cyber-physical WES is a point at which the cyber strategy and the switching controller satisfy the following two conditions.

(i) The cyber strategy pair $\{\bar{\mathbf{g}}, \bar{\mathbf{f}}\}$ is an NE of the cyber defense game $\mathbf{G}_c$ that corresponds to a power output profile $\{P_{ij}\}$, for $i, j \in \tilde{\mathcal{S}}$;

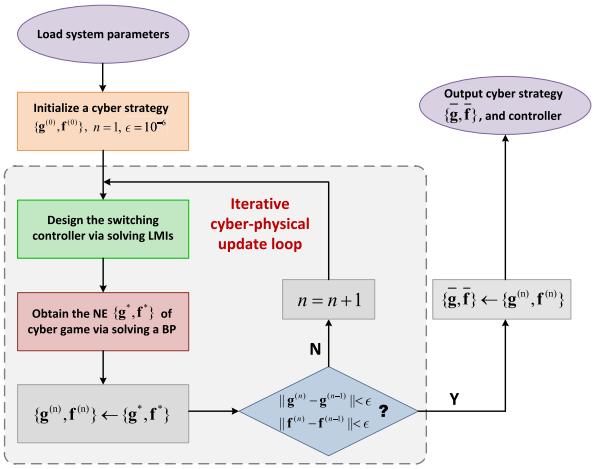


Fig. 6. A flow diagram of the iterative algorithm to obtain the system-of-systems equilibrium. The iterative loop contains the switching controller design for the physical layer and defense strategy update for the cyber layer.

(ii) Based on the state transition rates γ_{ij}, $i, j \in \mathcal{S}$, resulting from the cyber strategy $\{\bar{\mathbf{g}}, \bar{\mathbf{f}}\}$, the designed switching controller (13) *of WES yields a consistent power output profile $\{P_{ij}\}$ with the one in condition* (i)*, for $i, j \in \tilde{\mathcal{S}}$.*

The system-of-systems equilibrium requires one to design the WES's cyber and physical layers holistically.

B. Iterative Algorithm

To obtain the system-of-systems equilibrium, we develop an iterative algorithm based on solving the interleaving LMIs and BPs. For convenience, a flow diagram of the algorithm is shown in Fig. 6. We summarize the iterative algorithm in the following. First, we initialize a cyber strategy from (17), and determine the robust switching control of WES by solving LMIs (16). We update the game $\mathbf{G}_c$ as the utilities of attacker and defender are changed, and then recompute the NE strategy which further facilitates the next round of updates. Through a number of alternating updates of these two parts, the robust switching controller at the system-of-systems equilibrium is obtained, and the strategies of the game converge to $\bar{\mathbf{g}}$ and $\bar{\mathbf{f}}$ for the attacker and defender, respectively.

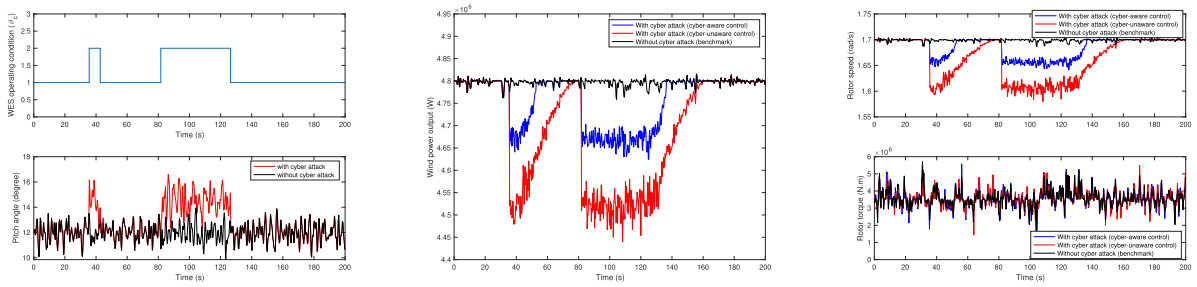
Comments on the Performance of the Algorithm and Its Implementation: The iterative cyber-physical update scheme is composed of two mappings. For convenience, we denote by μ the set of parameters of the physical controller that includes A_{Fi}, B_{Fi} and C_{Fi}, $i \in \mathcal{S}$. Thus, the first mapping from the cyber defense strategy to the physical controller can be denoted as $\mu = M_1(\mathbf{f}, \mathbf{g})$. Similarly, the other mapping from the physical controller to the cyber defense can be captured by $\{\mathbf{f}, \mathbf{g}\} = M_2(\mu)$. Note that M_1 and M_2 are two specific mappings determined by how the switching controller design and the strategic cyber defense mechanism are updated based on each other, as described in Fig. 6. One approach to show the convergence of the iterative algorithm is to use the small gain theorem [33, Chapter 5], i.e., showing the norm of the composed mapping $M_1 \circ M_2$ is smaller than 1, or equivalently $|M_1 \circ M_2| < 1$, where $|\cdot|$ is the standard Euclidean norm. Note that characterization of the closed-form expressions of M_1 and M_2 is challenging, as obtaining M_1 requires solving the LMIs in (16) and characterizing M_2 requires to compute NE by solving a BP. Thus, analyzing the convergence of the composed mapping $M_1 \circ M_2$ is highly nontrivial, which will be addressed in future work. We next provide a heuristic approach that can yield a converging iterative update trajectory with high confidence.

When implementing the designed iterative algorithm, we incorporate a small positive step size during the update of the resulting wind output power under the renewed cyber game equilibrium strategies. This procedure is similar to the classical gradient descent algorithm, in which a small positive learning rate is multiplied with the gradient value at the evaluated point. Our implementation can be seen as a cyber-physical gradient descent scheme. Specifically, the inclusion of this step size yields a cyber game with its entries at the next round of update close to its previous round, and this property also holds for the mixed strategy NE of the game. As such, the solutions to the LMIs will not deviate significantly between two consecutive updates, guaranteed by the convexity of the LMI constraints. To this end, the WES's performance (in the expected sense due to stochastic jumps) in a similar adversarial environment will not oscillate remarkably during the iterative updates, resulting in stable and converging trajectories of cyber strategies.

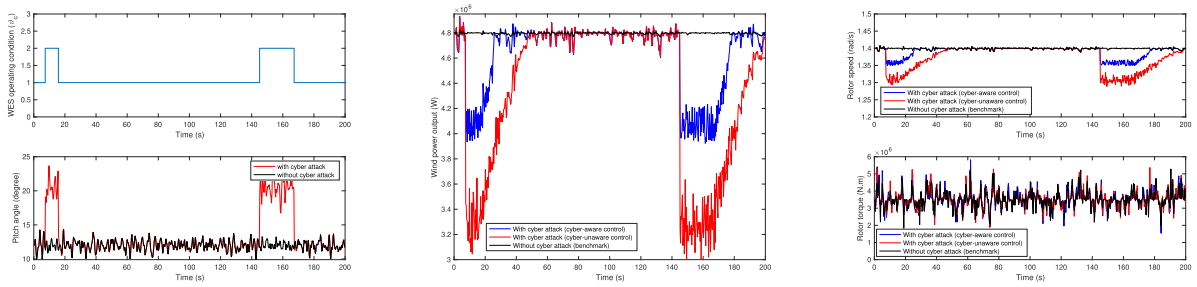
The computational complexity of the algorithm is also worth discussing. The proposed iterative algorithm mainly consists of two components: the switching controller design by solving LMIs and the cyber defense decision-making by computing the mixed strategy NE. To solve LMIs, one can use the well-developed Nesterov and Nemirovski's Projective Method (available in MATLAB through LMI toolbox), which has a polynomial-time complexity [34]. Computing the mixed strategy NE of the cyber game requires solving a bilinear program. One can leverage the widely used Lemke-Howson algorithm [35] which admits approximately a polynomial time complexity to achieve the goal. As the algorithm terminates in finite steps based on the above scheme, the proposed algorithm has polynomial time complexity. Another remark is that when the robustness parameter κ is very small (i.e., requesting a high-level of H_∞ noise attenuation), the LMIs may not admit a feasible solution. Thus, choosing an appropriate κ is necessary when designing the robust switching controller for the WES in implementation.

VII. Case Studies

We use case studies to corroborate the obtained results in this section. Specifically, we construct a WES with system parameters specified in [6]. The average wind speed is 15 m/s, and its disturbance is an independent and identical Gaussian distribution with a variance of 0.3. For illustrative clarity, we investigate two operation conditions without loss of generality, i.e., under normal operation and pitch angle sensor attack. Note that other attacks can be incorporated similarly. In the focused scenarios, the attacker corrupts the pitch angle sensor and injects a constant gain of 0.8 to the sensor value β. Thus, the control-aware cyber defense game is two-dimensional. We also assume that detecting the change of operating condition is agile, e.g., by analyzing the received



(a) WES operating condition and pitch angle. (b) WES output power. (c) Rotor speed and torque.



(d) WES operating condition and pitch angle. (e) WES output power. (f) Rotor speed and torque.

Fig. 7. (a) shows the operating condition of a WES in a certain period of time including the normal and pitch angle sensor attack states. (b) depicts the corresponding WES output power under the designed cyber-aware switching control together with cyber-unaware control for comparison. (c) shows the corresponding rotor speed and torque signals in different scenarios. (d)-(f) are counterparts to (a)-(c) where the attacker is more aggressive in compromising the pitch angle sensor signals.

time-series sensor information at the terminal control unit. And the magnitude of sensor corruption by the adversary can be inferred through the statistical difference between normal and compromised data using inference techniques. The following studies will show WES's robustness, security, and resilience in different scenarios and provide WES control design guidelines under the adversarial environment.

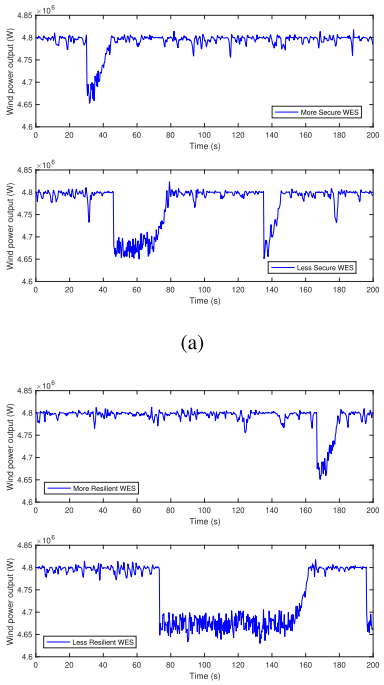
A. Cyber-Aware Robust Switching Control

We first corroborate the designed cyber-aware robust switching controller, and the robustness level is chosen as $\kappa = 10$ in (14). The results are depicted in Figs. 7(a)-7(c). Fig. 7(a) shows the sampled two-state Markov chain under the transition rate matrix $\Gamma = \begin{bmatrix} -0.003 & 0.003 \\ 0.1 & -0.1 \end{bmatrix}$, which governs the WES operating condition. Note that the values of transition rates vary across different energy systems, and they can be determined specifically by the historical data of the attack frequencies in targeted WES. Fig. 7(b) shows the WES output power using the designed control, and Fig. 7(c) presents the corresponding rotor speed and torque. For comparison, the WES performance under cyber-unaware robust control is also illustrated in which the controller only considers WES normal operation. The results show that the cyber-aware switching control outperforms the one without awareness significantly. The switching control is more efficient when the cyberattack happens since it incorporates this security consideration in the design beforehand. Based on the statistics [2], the monetary loss for a 50 MW wind farm using the designed cyber-aware control can be reduced by around 10k$ per month compared with the cyber-unaware counterpart, and this shows the advantages of the proposed methodology. We also conduct another case study that the attacker is more malicious by injecting a gain of 0.4 to the pitch angle sensor value. Such the attacker deceives the controller in measuring the correct pitch angle, and the applied control becomes inefficient. Note that the disruption caused by this attack case is significant, making it easy to be detected. The results are shown in Figs. 7(d)-7(f). It can be observed that the WES performance in terms of the generated power is worse than the previous case study under the attack. However, our developed cyber-aware robust switching control still outperforms the traditional cyber-unaware robust control.

B. Impact of Security and Resilience

We next investigate the impact of cybersecurity on WES performance. Specifically, we compare two cases in which the energy systems (WES 1 and WES 2) are with transition rates $\Gamma_1 = \begin{bmatrix} -0.001 & 0.001 \\ 0.1 & -0.1 \end{bmatrix}$ and $\Gamma_2 = \begin{bmatrix} -0.005 & 0.005 \\ 0.1 & -0.1 \end{bmatrix}$, respectively. Note that the cyber layer of WES 1 is more secure than that of WES 2 due to a smaller γ_{12}, while the resilience capabilities of the two systems are the same (same γ_{21}). The corresponding WES output power is shown in Fig. 8(a). We can see that WES 1 outperforms WES 2 in power generation efficiency, and thus a securer cyber system enhances the WES efficiency. This study suggests that if the system operator has more budget, he can invest more in the cyber layer of WES to reduce the risks of cyber system compromise.

To study the system resilience, we compare two scenarios in which the energy systems' transition rates are as follows: $\Gamma_1 = \begin{bmatrix} -0.001 & 0.001 \\ 0.1 & -0.1 \end{bmatrix}$ and $\Gamma_2 = \begin{bmatrix} -0.001 & 0.001 \\ 0.04 & -0.04 \end{bmatrix}$. These



(a)

(b)

Fig. 8. (a): WES performance under different cybersecurity levels. WES 1 outperforms WES 2 (i.e., with more output power) due to a higher security level. (b): WES performance under different resilience levels. The WES with a better resilience ability (former one) can generate more output power.

two systems are with the same level of security (same γ_{12}), while the former one is more resilient to attacks. The obtained result is shown in Fig. 8(b). We can see that the first WES can recover from the cyberattack more quickly than the latter, achieving better system performance.

In conclusion, increasing either γ_{21} or γ_{12} can improve WES efficiency. The system designer needs to strategically allocate a constrained amount of cybersecurity and physical restoration resources to obtain the desired outcome. This fact also demonstrates the tradeoff decision-making between system security and resilience.

C. Integrated Cyber-Physical WES Design

We next corroborate the effectiveness of the proposed iterative algorithm that yields a system-of-systems equilibrium design. Specifically, the cost parameters in the cyber game are assumed to be $C_{a,1} = 10\text{k\$}$ and $C_{d,1} = 5\text{k\$}$, and the weighting factor admits $\alpha = 10^{-2}\$/\text{W}$. We then compute the average generated renewable energy P_{ij} under the designed control for a given strategy pair $\{a_i, d_j\}$, $i, j \in \{0, 1\}$. Based on the iterative algorithm and the implementation procedure described in Section VI-B, Fig. 9 depicts the updated strategies of the defender and attacker in the control-aware cyber defense game. The cyber game strategies evolve iteratively by considering the physical WES performance. The algorithm successfully results in a system-of-systems equilibrium after several rounds of updates at which the players' strategies are $\bar{\mathbf{f}} = (0.224, 0.776)$ and $\bar{\mathbf{g}} = (0.895, 0.105)$, respectively. The results corroborate the effectiveness of the developed cyber-physical update scheme. This equilibrium strategy guides the strategic cyber defense of the WES operator by considering the physical system performance.

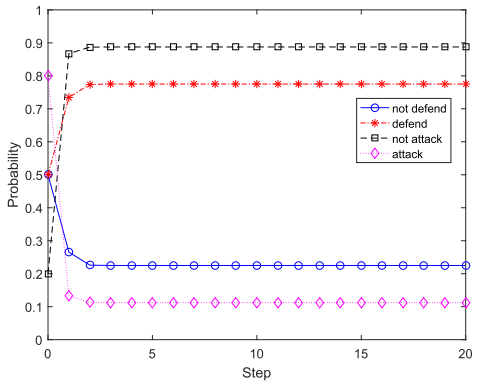


Fig. 9. Illustration of the iterative update algorithm. The algorithm converges to mixed strategies: $\bar{\mathbf{g}} = (0.895, 0.105)$ and $\bar{\mathbf{f}} = (0.224, 0.776)$ for the cyber attacker and defender, respectively.

VIII. Conclusion

This paper proposed a system-of-systems framework for the holistic design of cyber-physical WES that jointly considers system robustness, security, and resilience. We have provided a strategic defense mechanism using a non-cooperative cyber game for the cyber layer operator. We have further designed a switching controller for the physical WES operation, which has been corroborated to be robust and resilient. The system-of-systems equilibrium of the WES has been computed using an iterative mechanism by solving BPs and LMIs alternatively.

As for future work, we can explicitly quantify the values of robustness, security, and resilience of the designed system and use them for the optimal control design of cyber-physical WES under adversaries. One way to achieve this goal is to construct an objective function for the control design by incorporating costs related to system state, control input, and robustness (κ). One can further capture the costs of security (γ_{1i}, for $i \neq 1 \in \mathcal{S}$) and resilience (γ_{j1}, for $j \neq 1 \in \mathcal{S}$) in the constraint of the optimal control problem. For example, it is possible to use a linear combination between these two distinct metrics while considering budget constraints. The weighting factors in the combination represent the tradeoff between different metrics and can be determined accordingly based on the resulting WES performance and the system operator's preference.

References

[1] M. Ahmed and Y.-C. Kim, "Communication network architectures for smart-wind power farms," *Energies*, vol. 7, no. 6, pp. 3900–3921, Jun. 2014.

[2] GE. *GE Cybersecurity for Wind*. Accessed: Apr. 2019. [Online]. Available: https://www.ge.com/content/dam/gepower-renewables/global/en_US/downloads/brochures/ge-wind-cybersecurity.pdf

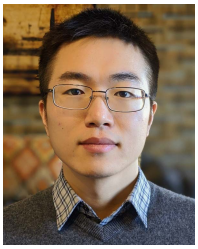
[3] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security Privacy*, vol. 9, no. 3, pp. 49–51, May 2011.

[4] R. Burkart, K. Margellos, and J. Lygeros, "Nonlinear control of wind turbines: An approach based on switched linear systems and feedback linearization," in *Proc. IEEE Conf. Decis. Control Eur. Control Conf.*, Dec. 2011, pp. 5485–5490.

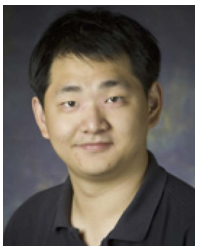
[5] B. Wu, Y. Lang, N. Zargari, and S. Kouro, *Power Conversion and Control of Wind Energy Systems*. Hoboken, NJ, USA: Wiley, 2011.

[6] P. F. Odgaard, J. Stoustrup, and M. Kinnaert, "Fault-tolerant control of wind turbines: A benchmark model," *IEEE Trans. Control Syst. Technol.*, vol. 21, no. 4, pp. 1168–1182, Jul. 2013.

[7] C. Shao, X. Wang, M. Shahidehpour, X. Wang, and B. Wang, "Security-constrained unit commitment with flexible uncertainty set for variable wind power," *IEEE Trans. Sustain. Energy*, vol. 8, no. 3, pp. 1237–1246, Jul. 2017.
[8] Y. Mo *et al.*, "Cyber–physical security of a smart grid infrastructure," *Proc. IEEE*, vol. 100, no. 1, pp. 195–209, Jan. 2012.
[9] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 998–1010, 4th Quart., 2012.
[10] W. U. Guangyu, J. Sun, and J. Chen, "A survey on the security of cyber-physical systems," *Control Theory Technol.*, vol. 14, no. 1, pp. 2–10, 2016.
[11] D. Wei, Y. Lu, M. Jafari, P. Skare, and K. Rohde, "An integrated security system of protecting smart grid against cyber attacks," in *Proc. Innov. Smart Grid Technol. (ISGT)*, Jan. 2010, pp. 1–7.
[12] N. Liu, J. Zhang, and W. Liu, "A security mechanism of web services-based communication for wind power plants," *IEEE Trans. Power Del.*, vol. 23, no. 4, pp. 1930–1938, Oct. 2008.
[13] T. Alpcan and T. Başar, *Network Security: A Decision and Game-Theoretic Approach*. Cambridge, U.K.: Cambridge Univ. Press, 2010.
[14] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Basar, and J. Hubaux, "Game theory meets network security and privacy," *ACM Comput. Surv.*, vol. 45, no. 3, p. 25, 2013.
[15] Y. Yuan, H. Yuan, L. Guo, H. Yang, and S. Sun, "Resilient control of networked control system under DoS attacks: A unified game approach," *IEEE Trans. Ind. Informat.*, vol. 12, no. 5, pp. 1786–1794, Oct. 2016.
[16] S. Rass, S. König, and S. Schauer, "Defending against advanced persistent threats using game-theory," *PLoS ONE*, vol. 12, no. 1, Jan. 2017, Art. no. e0168675.
[17] Q. Zhu and T. Basar, "Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: Games-in-games principle for optimal cross-layer resilient control systems," *IEEE Control Syst.*, vol. 35, no. 1, pp. 46–65, Feb. 2015.
[18] Y. Yuan, H. Yuan, D. W. C. Ho, and L. Guo, "Resilient control of wireless networked control system under denial-of-service attacks: A cross-layer design approach," *IEEE Trans. Cybern.*, vol. 50, no. 1, pp. 48–60, Jan. 2020.
[19] J. Chen and Q. Zhu, "Interdependent strategic cyber defense and robust switching control design for wind energy systems," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Jul. 2017, pp. 1–5.
[20] NIST. *Framework for Cyber-Physical Systems: Volume 1, Overview*. Accessed: Mar. 2022. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-201.pdf
[21] F. D. Bianchi, H. De Battista, and R. J. Mantz, *Wind Turbine Control Systems: Principles, Modelling and Gain Scheduling Design*. London, U.K.: Springer, 2006.
[22] K. E. Johnson, L. Y. Pao, M. J. Balas, and L. J. Fingersh, "Control of variable-speed wind turbines: Standard and adaptive techniques for maximizing energy capture," *IEEE Control Syst.*, vol. 26, no. 3, pp. 70–81, Jun. 2006.
[23] E. M. Herbert, *Hydraulic Control Systems*. Hoboken, NJ, USA: Wiley, 1967.
[24] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *Proc. 28th Int. Conf. Distrib. Comput. Syst. Workshops*, Jun. 2008, pp. 495–500.
[25] A. Teixeira, D. Pérez, H. Sandberg, and K. H. Johansson, "Attack models and scenarios for networked control systems," in *Proc. 1st Int. Conf. High Confidence Netw. Syst. (HiCoNS)*, 2012, pp. 55–64.
[26] D. P. D. Farias, J. C. Geromel, J. B. R. D. Val, and O. L. V. Costa, "Output feedback control of Markov jump linear systems in continuous-time," *IEEE Trans. Autom. Control*, vol. 45, no. 5, pp. 944–949, May 2000.
[27] P. Seiler and R. Sengupta, "Analysis of communication losses in vehicle control problems," in *Proc. Amer. Control Conf.*, vol. 2. 2001, pp. 1491–1496.
[28] O. L. V. Costa, M. D. Fragoso, and R. P. Marques, *Discrete-Time Markov Jump Linear Systems*. London, U.K.: Springer, 2006.
[29] H. Ghadiri, M. R. Jahed-Motlagh, and M. B. Yazdi, "Robust stabilization for uncertain switched neutral systems with interval time-varying mixed delays," *Nonlinear Anal., Hybrid Syst.*, vol. 13, pp. 2–21, Aug. 2014.
[30] H. Ghadiri and M. R. Jahed-Motlagh, "LMI-based criterion for the robust guaranteed cost control of uncertain switched neutral systems with time-varying mixed delays and nonlinear perturbations by dynamic output feedback," *Complexity*, vol. 21, no. S2, pp. 555–578, Nov. 2016.
[31] H. Ghadiri, M. R. Jahed-Motlagh, and M. B. Yazdi, "Robust output observer-based guaranteed cost control of a class of uncertain switched neutral systems with interval time-varying mixed delays," *Int. J. Control, Autom. Syst.*, vol. 12, no. 6, pp. 1167–1179, Dec. 2014.
[32] T. Başar and G. J. Olsder, *Dynamic Noncooperative Game Theory*, vol. 23. Philadelphia, PA, USA: SIAM, 1999.
[33] H. K. Khalil and J. W. Grizzle, *Nonlinear Systems*, vol. 3. Upper Saddle River, NJ, USA: Prentice-Hall, 2002.
[34] Y. Nesterov and A. Nemirovskii, *Interior-Point Polynomial Algorithms in Convex Programming*. Philadelphia, PA, USA: SIAM, 1994.
[35] L. S. Shapley, "A note on the Lemke–Howson algorithm," in *Pivoting and Extension*. Berlin, Germany: Springer, 1974, pp. 175–189.



Juntao Chen (Member, IEEE) received the B.Eng. degree (Hons.) in electrical engineering and automation from Central South University, Changsha, China, in 2014, and the Ph.D. degree in electrical engineering from New York University (NYU), Brooklyn, NY, USA, in 2020. He is currently an Assistant Professor at the Department of Computer and Information Sciences and an affiliated Faculty Member with the Fordham Center of Cybersecurity, Fordham University, New York City, NY, USA. His research interests include cyber-physical security and resilience, game and decision theory, network optimization and learning, artificial intelligence, and equitable smart cities. He was a recipient of the Ernst Weber Fellowship, the Dante Youla Award, and the Alexander Hessel Award for the Best Ph.D. Dissertation in electrical engineering from NYU.



Quanyan Zhu (Member, IEEE) received the B.Eng. degree (Hons.) in electrical engineering from McGill University in 2006, the M.A.Sc. degree from the University of Toronto in 2008, and the Ph.D. degree from the University of Illinois at Urbana-Champaign (UIUC) in 2013.

From 2013 to 2014, he was a Post-Doctoral Research Associate at the Department of Electrical Engineering, Princeton University. He is currently an Associate Professor with the Department of Electrical and Computer Engineering, New York University (NYU). He is also an affiliated Faculty Member with the Center of Cyber Security and the Center for Urban Science and Progress, NYU. His current research interests include cyber-physical systems, cyber security and deception, game theory, machine learning, and network optimization and control. He was a recipient of many awards including the NSF CAREER Award, the NSERC Canada Graduate Scholarship (CGS), the Mavis Future Faculty Fellowships, and the NSERC Postdoctoral Fellowship (PDF).