IEEE TRANSACTIONS ON
SMART GRID

http://ieeexplore.ieee.org/Xplore

Power System Reliability Assessment Incorporating Cyber Attacks Against Wind Farm Energy Management Systems

Yichi Zhang, Yingmeng Xiang, and Lingfeng Wang

Abstract—**By exploiting the vulnerabilities in cyber components, an attacker could intrude into the wind farm supervisory control and data acquisition (SCADA) system and energy management system (EMS) and maliciously trip one or multiple wind turbines. The reliability of the overall power system could thus be impacted by the performance of wind farms. In this paper, cyber attack scenarios concerning cyber components or networks are considered in the integrated wind farm SCADA/EMS system architecture. Two Bayesian attack graph models are adopted to represent the procedures of successful cyber attacks, and a mean time-to-compromise model is used by considering different attack levels and various vulnerabilities. Frequencies of successful cyber attacks on the wind farm SCADA/EMS system are estimated. A procedure for evaluating the power system reliability is proposed by considering wind turbine trips caused by various cyber attacks. Simulations are conducted based on a typical IEEE reliability test system. Simulation results indicate that the overall system reliability decreases when the frequency of successful attacks on the wind farm SCADA/EMS system and skill levels of attackers increase.**

Index Terms—**Cyber security, cyber-physical power systems, wind farm energy management system, power system reliability, Bayesian attack graph model, mean time-to-compromise, expected energy not supplied, loss of load probability.**

NOMENCLATURE

ARMA(m, n)	Autoregressive Moving Average model with m autoregressive terms and n moving average terms.
AGC	Automatic Generation Control
BMW	Bear Mountain Wind
CPS	Cyber-Power System
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
DERFEM	Duality Element Relative Fuzzy Evaluation Method
DB	Database
DMZ	Demilitarized Zone
EENS	Expected Energy Not Supplied
EMS	Energy Management System
GDA	Grid Data Acquisition
HTTP	Hyper Text Transfer Protocol
ICCP	Inter-Control Center Communications Protocol
ICT	Information and Communications Technology
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
LAN	Local Area Network
LOLP	Loss of Load Probability
MCS	Monte Carlo Simulation
MITM	Man-in-the-Middle
MTTC	Mean Time-to-Compromise
MTTR	Mean Time-to-Repair
NFS	Network File System
PDI	Process Data Interface
PLC	Programmable Logic Controller
POI	Point of Interconnection
RFE	Redundant Front Ends
RTS 79	IEEE Reliability Test System 79
RTU	Remote Terminal Unit
RSH	Remote Shell
SCADA	Supervisory Control and Data Acquisition
SCU	Substation Control Unit
SG	Sub-Goal
SITL	System-in-the-Loop
SSH	Secure Shell
SSL	Secure Socket Layer
SSMARS	System Stability Monitoring and Response System
VCS	Voltage Control System
VPN	Virtual Private Network
WAMS	Wide Area Measurement Systems
WAN	Wide Area Network
WTCP	Wind Turbine Control Panel
WTCS	Wind Turbine Control System
α_t	Normal white noise at time t
C	Condition
CM	Countermeasure
DB	Database
$https$	Hyper Text Transfer Protocol over Secure Socket Layer
L	Privilege
N	Connection
nfs	Network File System

This work was supported by the National Science Foundation (NSF) under Award ECCS1128594.

Y. Zhang is with the Department of Electrical Engineering and Computer Science, University of Toledo, Toledo, OH 43606, USA.

Y. Xiang and L. Wang were with the Department of Electrical Engineering and Computer Science, University of Toledo, Toledo, OH 43606, USA. They are now with the Department of Electrical Engineering and Computer Science, University of Wisconsin-Milwaukee, Milwaukee, WI 53211, USA (e-mail: l.f.wang@ieee.org).

Digital Object Identifier: 10.1109/TSG.2017.2523515

OG	Overall Goal
$P1$	Probability that the attacker is in process 1
rsh	Remote Shell Service
S	Service
ssh	Secure Shell
T	Overall Compromise Time
t_1, t_2, t_3	Expected Time in Process1, 2, and 3
u	Probability of the Unsuccessful Process 2
V	Vulnerabilities
y_t	Value of the time-series at time t
$\emptyset_i,\ \theta_j$	The i_{th} autoregressive parameter and the j_{th} moving average parameters
σ_a^2	Deviation of the white noise
SW_t	Simulated wind speed at time t
μ_t, σ_t	Mean value and standard deviation of the observed wind speeds at time t
P_r	Rated power of the wind turbine
V_{ci}, V_r, V_{co}	Cut-in speed, rated speed and cut-out speed of the wind turbine
τ_1, τ_2, τ_3	Constants for calculating wind power
$V_a\,(t)$	System security index at time t
$P_{gen}\,(t)$	Total conventional generation at time t
$P_{load}\,(t)$	Total load demand at time t
P_w	Wind turbine power output
$\Delta P_{attack}(t)$	Wind power that can be tripped by the attackers at time t
$n_{turbine}$	Number of wind turbines
t_c	Time-to-compromise
t_r	Time-to-repair
U	A random number within [0, 1]

I. Introduction

The utilization of the renewable energy is increasing rapidly and steadily in recent years. In 2013, all renewable energy resources have delivered about 13% of the electricity in the U.S., and the wind power takes about 4.13% of the electricity generation and has become the fifth largest electricity source. In Iowa and South Dakota, wind power has exceeded 25% of the total electricity production. Texas owns the largest installed wind capacity and its electricity generation from the wind energy is 35.9 million MWh, which is enough for supplying 3.3 million homes [1].

With the development of wind turbine technology, large scale wind farms are being developed in many countries. It is anticipated that 20% of U.S. electricity will be provided by the wind energy, which will be 5.8 billion MWh by 2030 [2]. The wind farms might be enabled with the control capabilities of a power plant [3]. With the increased and concentrated penetration of wind power into the power grid, the power grid nowadays is becoming more dependent on the wind energy production, and the performance of the overall power system will be inevitably affected by the operations of wind farms [4].

Information and communications technology (ICT) is important for the coordination between wind farms and the power system. The supervisory control and data acquisition (SCADA) system and energy management system (EMS) are crucial in monitoring, operating, and protecting both wind farm generators and the power system [3]. The wind farm SCADA can be used to configure and modify parameters of the individual physical component or the whole wind farm. It may also optimize the timer, and force machines to operate in particular modes, such as operating the machines at lower power [5]. Wind power companies may own multiple wind farms and could integrate them into a single wind farm EMS, where the main control is from the control center through the control wide area network (WAN) [4].

Cyber attacks are emerging threats to the modern power systems. Power system network has become an attractive target of the malicious groups and individuals. For instance, it is reported that the National Grid is under the minute-by-minute threat of cyber attacks, [6]. The SCADA/EMS is of specific concern among the cyber systems in the power system. By attacking the SCADA/EMS system, the performance of the power system may be impacted. Malicious code such as Stuxnet has successfully intruded into the industrial SCADA system and resulted in severe impacts [7]. As more zero-day vulnerabilities are being exploited, control systems may be attacked without noticing the vulnerability exploits. This will bring more serious impacts to the power system [8]. Reference [9] estimated the impact on the SCADA system brought by the data integrity attacks. With successful attacks on the Automatic Generation Control (AGC) loop, the magnitude of the load generation imbalance indicates severe impact could be brought to the AGC of the power system. In [10], possible cyber attacks that may occur on devices of industrial control systems are considered. These cyber attacks are also classified based on their impacts on the key control loops in the power system.

Cyber attacks on the wind farm SCADA/EMS systems may result in widespread disruptions of electric power systems considering the rapidly increasing penetration of wind power. Therefore, investigations on the cyber security of the wind farm SCADA/EMS systems are much needed [4]. With higher integration of wind generation, as well as the advanced cyber components and networks, cyber attacks against the wind generation will become a non-negligible factor which could influence the proper operations of wind turbines. It is crucial to account for the attacks against the wind generation when evaluating the overall power system reliability. However, limited work associated with this critical topic has been conducted so far.

In this paper, quantitative evaluation of the cyber attack on the wind farm SCADA/EMS is carried out. A modified Bayesian attack graph model is used to describe the intrusion processes into different wind farm SCADA/EMS networks. A mean time-to-compromise (MTTC) model [11] is used for estimating average time intervals of successful attacks on targeted cyber components in the wind farm SCADA/EMS system. MTTCs consumed on vulnerability exploits in wind farm SCADA/EMS networks are calculated, and frequencies of successful attacks on the targeted cyber components are evaluated. Wind turbines are tripped when false commands are sent through the penetrated cyber components. With a forensic mean time-to-repair (MTTR) of the intruded cyber component, probabilities of successful cyber attacks against the wind farm SCADA/EMS system are calculated. By sending the unauthorized trip commands to wind turbines or wind farms after successful intrusions, breakers of the power system are forced to trip, which leads to increased outage intervals of physical components. Finally, Monte Carlo simulation (MCS) is used to perform the reliability analysis of the power system.

The major contributions of this paper are summarized as follows: (1) Quantitative analysis is conducted to investigate the MTTCs of the wind farm related control systems. (2) To the best of our knowledge, this is the first paper which includes cyber attacks against wind generation in wind integrated power system reliability evaluation.

The remainder of the paper is organized as follows. In section II, the related work of cyber attacks on common and wind farm SCADA/EMS systems is reviewed, and research challenges on wind farm SCADA/EMS are considered. In section III, the architecture of the wind farm SCADA/EMS system is proposed, and five cyber attack scenarios on the wind farm SCADA/EMS system are described. In Section IV, two Bayesian attack graph models and the MTTC model are discussed. In section V, the wind speed is modeled, which is integrated into the power system reliability model. In section VI, with the attack graph and MTTC models, time intervals of successful cyber attacks on different wind farm SCADA/EMS components are calculated. And the reliability of the power system is evaluated considering various cyber attacks on the wind farms. The expected energy not supplied (EENS) and loss of load probability (LOLP) values for IEEE reliability test system 79 (RTS79) are estimated based on the MCS. Finally, the paper is concluded in section VII.

II. Related Work

A. Quantitative Assessment of Cyber Threats on the SCADA/EMS System

A number of quantitative methods on the vulnerability assessment have been proposed for the SCADA/EMS system. For instance, in [12], a risk assessment framework is proposed to enhance the robustness of the power system against cyber attacks. The vulnerability of the cyber system is evaluated with the Duality Element Relative Fuzzy Evaluation Method (DERFEM), and the attack scenarios are illustrated with the attack graph. With the System Stability Monitoring and Response System (SSMARS), the impact of intrusions on the power system is monitored in real time, and the power system stability is evaluated. And [13] proposes a cyber-physical test bed by integrating the Real-Time Digital Simulator (RTDS) power grid simulator and the Opnet's System-in-the-Loop (SITL) simulator. Two cyber attacks on the communication protocol of the SCADA system are discussed, and vulnerabilities in the cyber-physical system are evaluated in real time. In [14], a co-simulation framework called cyber-power system (CPS) tool is proposed. The communication between the SCADA system, the power system, and the transmission operator is simulated. Cyber attacks at the cyber layer and the impact on the power system layer are analyzed in the real-time and industrial simulation environment.

B. ICT in the Wind Farm SCADA/EMS System

Communication systems are widely used in the power grid with the integration of the renewable energy generators. A number of equipment and devices in the power grid are monitored and controlled by the advanced communication technologies, and the crucial decision-making support systems and applications such as SCADA and EMS are in place. Both renewable energy generators and power grid can be monitored and protected by the ICT applications. Several studies have been performed on the application of the ICT on the wind farm SCADA/EMS system. For instance, in [3], communication technologies for wind power integrated grid, such as power line communications and wireless local area networks, are reviewed. Meanwhile, a realistic renewable energy project is analyzed based on the communication systems in Bear Mountain Wind (BMW) farm. Reference [10] proposes typical communication architectures of the local wind farm control and the wind control center. Functionalities and devices of the wind control center and other control centers are compared. In [15], the offshore wind farm is considered as a local area network (LAN), and LAN access techniques such as Ethernet and International Organization for Standardization (ISO) models are integrated into the offshore wind power system. Reference [16] discusses the communication technologies in the wind turbine control system (WTCS) and wind park control system. It was found that the wind park communication network adopts the switching techniques and Carrier Sense Multiple Access with Collision Detection (CSMA/CD) network access method. And an interactive cyber-based protocol between the power system and the wind farm was proposed in [17], where the interactive protocol between transmission networks and the wind generator module leads to a system-wide stable operation.

C. Vulnerability Assessment on the Wind Farm SCADA/EMS System

It is crucial to quantitatively evaluate the impact brought by the cyber vulnerabilities and attacks on the wind farm SCADA/EMS system. However, limited work associated with this pressing topic has been conducted so far. In [4], three architectures of wind farm SCADA networks are proposed, and vulnerabilities and potential cyber attacks on the SCADA system of the wind farm are identified. Various cyber intrusion scenarios are considered on the wind farm SCADA system, and the impacts on power system dynamics brought by cyber attacks are analyzed. Reference [18] proposes a cyber security architecture for the wind farm connected power grid. Secure communication of wind connected electric grid is discussed, and data transmission and virtual private network (VPN) are considered to evaluate the impact brought by cyber attacks on wide area measurement systems (WAMS). A comprehensive vulnerability branch assessment indicator of the wind farm connected power grid is proposed in [19]. Static energy function and complex network theory are used to model the assessment indicator. The indicator is adopted on the double-fed wind farms, which are contained in the IEEE-30 bus system. It is found that access points of the wind farms and vulnerabilities of branches in the power grid could impact each other in an interdependent manner.

D. Power System Reliability Evaluation Associated with Wind Energy

Power system reliability evaluation is to estimate the capacity and adequacy of the power system for supplying power to the customers with the desired quality of service. The deployment of wind energy in a smart grid environment inevitably has a significant influence on the power system reliability. In [20], the generating capacity of the power system is evaluated including wind energy. In [21], polulation-based intelligence search is used to accelerate the reliability evaluation of power grid with wind energy peneration. In [22], the fundamental factors, models and methods related to wind integrated system reliability evaluation are analyzed and compared. These studies focus on the physical impacts of the wind energy, while the cyber vulnerabilities are not considered.

E. Research Challenges in Wind Farm SCADA/EMS System

Compared with the common SCADA/EMS in the bulk power system, more vulnerabilities and unauthorized accesses are involved in the wind farm SCADA/EMS. Possible attacks and corresponding countermeasures should be considered concerning the additional vulnerabilities. For instance, the wind turbine control panel (WTCP) of the wind farm is able to control and monitor the status of wind turbines, whereas it possesses limited cybersecurity capabilities to prevent or mitigate the cyber intrusions, thus it can be considered as an additional unauthorized access point of the intrusion into the wind farm SCADA/EMS [4]. Also, optical fibers are heavily used in the communication of wind farms. However, by using the advanced tapping method such as injecting additional light into the fibers, measurement and commands between the control center and wind farm substations could be modified. Thus the data encryption approaches and fiber intrusion detection system (IDS) are needed to ensure the cybersecurity of the wind farm.

In [3], research challenges in communication of wind farm SCADA are discussed. Robust two-way communication technologies should be developed, and capabilities of the wind farm SCADA, such as wind energy efficiency and control speed, can thus be improved. Severe security hazards may be caused by an energized electrical island, an efficient detection system is thus needed to fix the islanding problem. Wireless and programmable logic controller (PLC) technologies are proposed in [3] as approaches for island detection. At the same time, due to the distributed networks of the wind farms, wireless technologies of the wind farm SCADA/EMS are necessary for monitoring, authorization, and control. Also, wind energy is highly unstable and intermittent, dynamic control of the power system should be in real-time and accurate, thus more efficient and reliable communication systems are needed for the synchronized phasor and data management of the wind energy. Finally, standardization of communication protocols in the wind farm SCADA/EMS is necessary, so that wind farms can be controlled and monitored more efficiently [3].

III. Cyber Attack Scenarios on the Wind Farm EMS

A. Architecture of the Cyber Network in the Wind Farm EMS

Fig. 1 illustrates the representative architecture of the wind farm SCADA/EMS system, which is used to control and monitor the generation and distribution of the wind power. In Fig. 1, the network of the wind farm SCADA/EMS is divided into five sub-networks: wind farm local control LANs, the wind farm main control center LAN, the backup remote control LAN, and communication links which connect the LANs through the control WAN.

The wind farm local control LAN is either a stand-alone wind farm SCADA network in the control room, or a partially integrated network which integrates the corporate network for business [4]. In this study, only the stand-alone wind farm SCADA network is considered, which is used to provide the monitoring and control functions for the wind turbines in one farm. In the local control LAN, communication protocols implemented in wind farm communication networks are International Electrotechnical Commission (IEC) 61400-25, which provides the SCADA system with the ability to communicate with any device in a standard approach [23]. The real-time command and measurement information are presented on the workstation, and the long-term data received from the measurement components are stored in the historical database. The wind farm SCADA performs the function of acquiring the grid data, which are the measured electrical variables at the wind turbines. For instance, the METEO function installed in the wind farm SCADA is used for collecting meteorological data such as wind speed and temperature. The monitored wind farm data are processed by the SCADA server and transmitted to the application server. Through the workstation, the operators are able to monitor the electrical states and modify parameters of the physical components in the wind farm [3]. Unauthorized user may intrude into the local control LAN and control the workstation, thus malicious command may be sent to turn off the wind turbines or change the parameters of the controller.

In the wind farm main control center, there are multiple units of redundant front ends (RFEs) in the hot standby mode. These RFEs are used for receiving and delivering the information from or to the wind farms. The information of each wind farm is stored in the servers of the corresponding RFE temporarily and will be updated with the constant frequency. There are M units of control center operator consoles to present the information acquired by the RFEs. And the intruders may send the unauthorized operation or dispatch commands to different wind farms. The video wall exhibits the graphical output, which acquires state information of the wind farms from the consoles. Two historian servers are used for restoring historical data, which are received from the front ends or the wind farms. The redundant hard disk can be accessed by both servers so that the availability of historian data acquisition can be improved. The web server stores the real time and historical information through the remote clients [23]. The Inter-Control Center Communications Protocol (ICCP) server is able to respond to requests of data exchange from other ICCP clients in the backup remote control

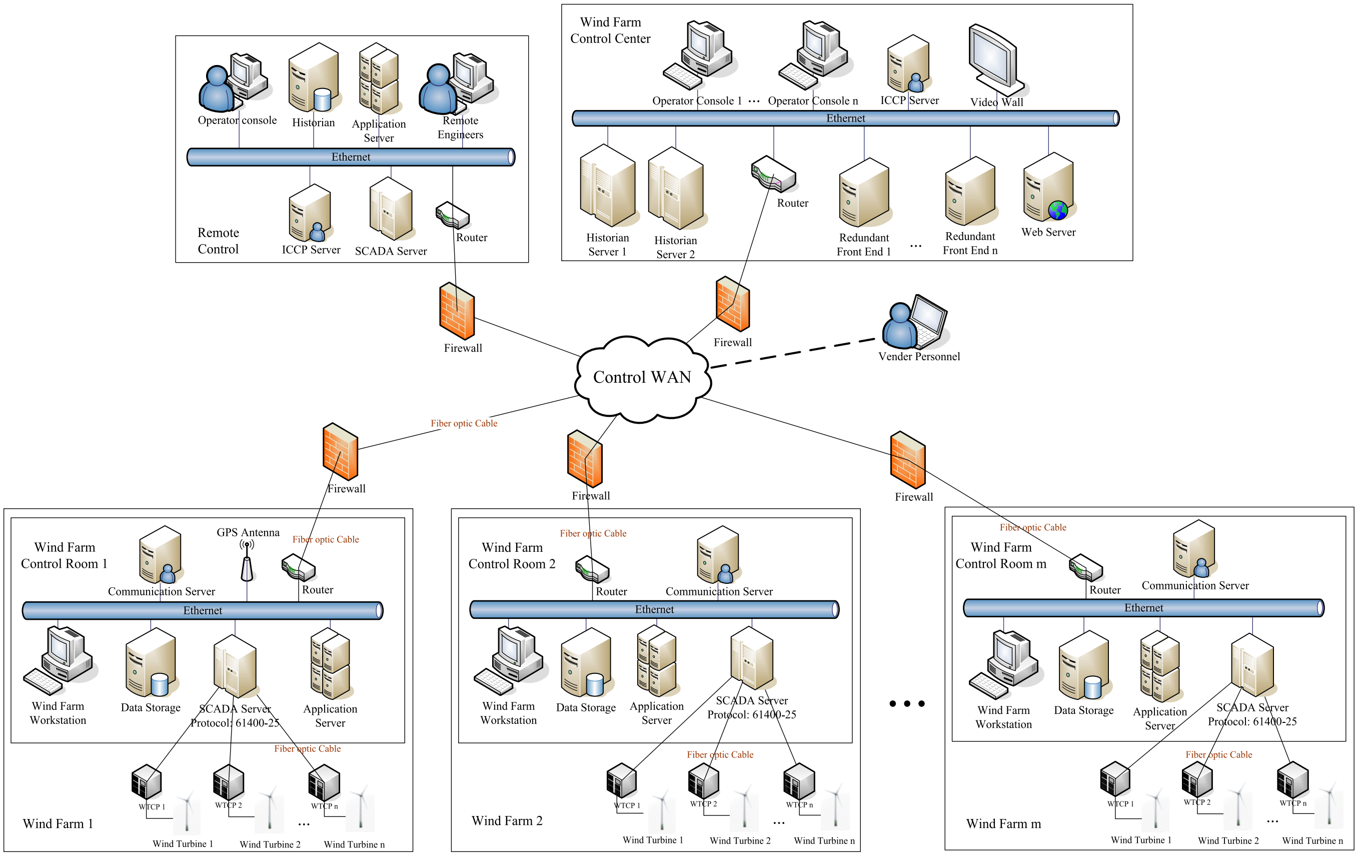

Fig. 1. A representative wind farm SCADA/EMS architecture.

centers. Multiple separated wind farms are integrated and monitored by the EMS installed in the wind farm control center. The wind farm control center EMS is able to regulate the voltages of wind turbines, coordinate the outputs of the wind farms, and provide the reactive power support for the utility system [24]. The backup remote control center LAN is considered as the backup of the main control center LAN, and it is able to control the remote SCADA system of the wind farms.

In order to effectively manage a large number of wind farms from one control center, two protocols (i.e., IEC 61850-7 and IEC 61400-25) are developed. With these protocols, a common communication architecture for monitoring substations and controlling wind farms can be realized. A standardized communication protocol is used between networks in the SCADA/EMS system. Common communication protocols of wind farm substations are IEC 60870-5-101, DNP 3.0, Modbus remote terminal unit (RTU) and TCP [10]. Energy meters are used to record the energy data and verify the energy consumption. Energy meters are connected to a serial bus, which is linked by a serial-Ethernet adapter to the wind farm SCADA/EMS system. Energy data are downloaded to the meter via IEC 60870-5-102 over Ethernet or other standard protocols. Protocols among wind turbines are usually not standard. In order to prevent the third parties from controlling communications of the wind turbines or overriding the wind farm SCADA, wind turbine manufactures usually define their own protocols for wind turbine PLCs [10].

Since the wind farms are additional resources to the power systems, besides wind farms and wind turbines, remote control is the additional difference between wind farm SCADA/EMS and the usual SCADA/EMS. The SCADA remote control is used for remotely monitoring data of the wind farm, and authorized users are allowed to access the SCADA database and modify parameters of the data controller [3]. At the same time, modules in the wind farm SCADA/EMS specifically designed for wind energy measurement and commands are different from the common SCADA system. For instance, in Fig. 2, communication system and interface of the BMW wind farm SCADA are designed based on communications between substations and wind farms [3].

In the modules of the BMW wind farm SCADA system [3], the SCADA REMOTE module is used for monitoring data from the wind farms, and controller parameters can be modified in the SCADA database through this module. Real-time wind farm data is exchanged through the process data interface (PDI), and electrical variables are measured from the point of interconnection (POI) substation by using the grid data acquisition (GDA) module. Meanwhile, electrical states are monitored and remote switching operation is transmitted by the substation control unit (SCU) in the wind farm substation. Dynamic voltage at the POI substation can be controlled by the voltage control system (VCS), which can use reactive power capability of wind turbines online. And the METEO module is

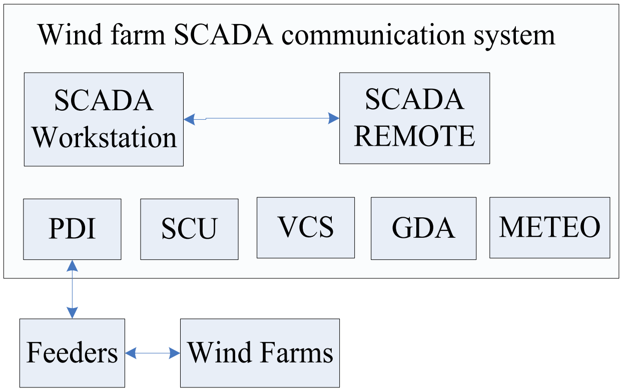

Fig. 2. Wind farm SCADA communication system.

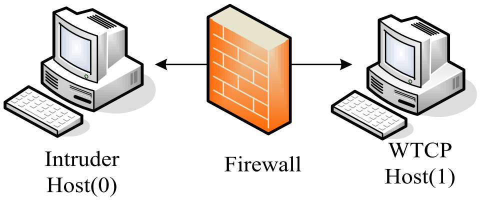

Fig. 3. Cyber attack on WTCP.

utilized for collecting meteorological data, such as wind speed and direction, and temperature. All status and measured data are transmitted with the standard protocol, such as IEC 60870-5-10, through the SCADA system. Status data are updated at most four times per second.

B. Cyber Attack Scenarios and Paths to Wind Farm EMS

When the attacker has successfully intruded into the wind farm SCADA/EMS system, false commands such as trip commands will be launched from the target components, and the wind turbines will thus be stopped. As a result, the reliability of the whole power system will be impacted. Different network configurations in the wind farm SCADA/EMS and intrusion steps of the targeted components are discussed in the following.

1) *Attack on WTCP:* WTCP is a control and monitoring unit with the display screen and operating keys. Besides acquiring the instantaneous operating status and measurement values of the wind turbines, operations of configuration to the connected wind turbine can be performed through one WTCP [4]. Since the WTCP is normally mounted on the tower base and is easily accessible, it is not difficult to be accessed by unauthorized attackers. Thus it can be considered as the easiest target for the attacker. It is assumed the attacker is able to directly reach the WTCP by bypassing the firewall. By exploiting vulnerabilities in the WTCP, or by cracking the pin of the WTCP [4], the attacker is able to connect his intrusion device to the WTCP. Then he may gain the control privilege of the WTCP by using the buffer overflow attack, and malicious commands can be sent to the wind turbine controlled by the intruded WTCP. The intrusion process is illustrated in Fig. 3.

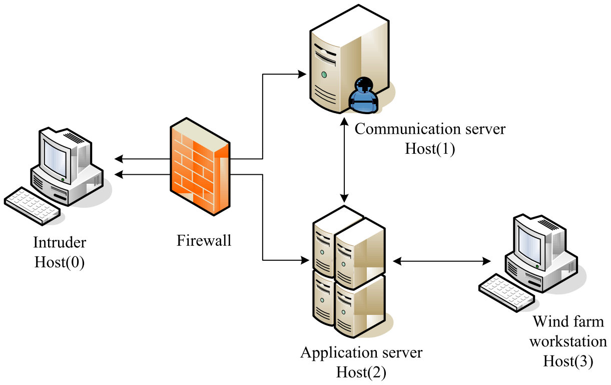
Communication server Host(1)
Intruder Host(0)
Firewall
Application server Host(2)
Wind farm workstation Host(3)

Fig. 4. Cyber attack on wind farm local control LAN.

2) *Attack on Local Control LAN of One Wind Farm:* Internal attack is possible on various LANs of the wind farm SCADA/EMS system, the attacker may obtain the physical access to the LAN and send the unauthorized command, but in this study, it is assumed that all attacks are launched from outside networks. By exploiting vulnerabilities in the component which is able to communicate with the Ethernet, the attacker is able to intrude into various internal LANs of the wind farm SCADA/EMS system. In the next step, by exploiting vulnerabilities of the services executed on the intermediate component, the attacker intrudes into the cyber device connected to the firstly compromised component. The targeted component can thus be reached by exploiting corresponding vulnerabilities. If the targeted component is reached, the intruder will upgrade his privilege by using buffer overflow attack. When the attacker finally possesses the root privilege, the commands will be sent to the wind turbines.

The attack target in the wind farm control room is the wind farm workstation. The network configuration and the attack process are shown in Fig. 4. When the attacker has successfully intruded into the control room by bypassing the firewall, he needs to intrude into either the communication server or the application server. The communication server, which is similar to the ICCP server, is used to process the information retrieved from or sent to the control center, and it is not allowed to directly communicate with the workstation [25]. The application server stores the measurement data in the real-time database, and it transmits control commands to the workstation. When the attacker has gained the privilege to control the workstation, wind turbines controlled by the wind farm being attacked will receive the fabricated trip commands and be forced to stop.

1) *Attack on Wind Farm Backup Remote Control LAN:* The remote control center is used to coordinate the main control center, so that remote monitoring and control on the wind farms can be realized. In Fig. 5, the attack procedure on the remote control LAN is illustrated. Since the remote control is used to communicate with

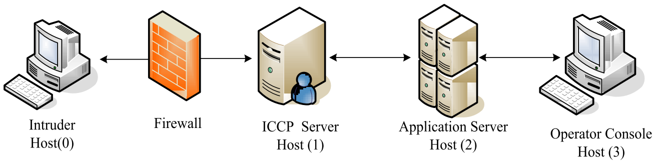

Fig. 5. Cyber attack on wind farm backup remote control LAN.

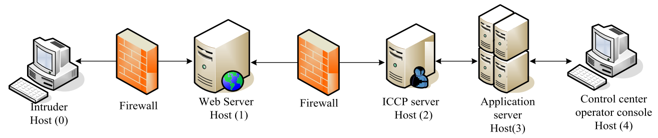

Fig. 6. Cyber attack on wind farm control center LAN.

the main control center, no web server is installed in the remote control LAN. The attacker can access the remote control network when the firewall is bypassed, then he is able to intrude into the ICCP server. By exploiting the vulnerabilities in the application server connected to the ICCP server, and obtaining its user privilege. The intruder will finally access the operator console and send trip commands with a permitted identity.

1) *Attack on Wind Farm Control Center LAN:* Fig. 6 illustrates the network configuration and the attack on the control center LAN. The attacker needs to intrude into the web server, which may be installed in the demilitarized zone (DMZ) of the network. When the attacker has bypassed the second firewall which separates the DMZ and the control center LAN, he needs to successfully reach the ICCP server, which is used for communications with the backup control centers. The remaining steps are similar to the attacks on the backup remote control LAN, which are obtaining the user privileges of the application server and the operator console. Compared with the intrusion into the backup remote control LAN, it should be noticed that the attacker needs to exploit different vulnerabilities in the control center LAN.
2) *Attack on Communication Links of Wind Farms:* Communication links that may be attacked in the SCADA/EMS are those between the control center LAN and the wind farm local control LAN, as well as the links between WTCPs and wind turbines. The man-in-the-middle (MITM) attack can be launched to the communication links. Since optics fibers are mostly used as the material of the wind farm communication links, by installing surreptitious taps on the optical fiber cable, additional light and fake information can be injected to the communication links [4]. Also, the attacker may obtain necessary information by eavesdropping and analyzing the light information. With traffic monitoring and analysis in the communication links, the attacker may understand the traffic patterns, and the data of fake measurement will be sent to the operators in the main wind control center or local control room. Finally, malicious control commands will be sent from operators to wind turbines [4].

In all attack scenarios mentioned above, after the attacker gains the desired control privellige, he can perform cyber attacks in multiple ways, such as stealing the information, shutting down the wind turbines, disrupting the voltage, and interrupting the power system operation. In some extreme cases, the wind turbine could be physically damaged, though it is a rather difficult task considering the associated monitoring and protection functionalities. This paper focuses on the long-term power system relibility whose analysis is mainly concerned with the working statuses of the wind turbines. If a wind turbine is tripped, its status will become down, which will cause the decrease of total generation capacity and may result in load loss. This is a major way for wind turbines to impose negative effect on the power system and it is normally more detrimental than the information loss. Besides directly tripping the wind turbines, attackers with advanced skills can control the wind turbines and disrupt the frequency or voltage. As the operation of wind turbines is continuously monitored by the control center, wind turbines will be tripped by the power system operator if they are operating abnormally. In short, the wind turbines could be directly or indirectly tripped due to the cyber attacks, and as a result detrimental impact will be caused to the power system operation.

IV. Cyber Attack Model of Wind Farm EMS

A. Bayesian Attack Graph Models and Probabilities

Fig. 7 illustrates a Bayesian attack graph model of vulnerabilities in the wind farm control center LAN, which is the minimal attack path to the root privilege of the operator console. In the attack graph $G(V \cup C)$, two types of nodes are considered: exploit to vulnerability V and component condition C. The condition is distinguished as service (S), which is shown as $servise(host)$; the connection (N) is represented as $< sourcehost, destinationhost >$; and the privilege ($L$) is denoted as $privilege(host)$. An exploit is executed only if all its pre-conditions are satisfied, and a condition can be the post-condition of an exploit, or satisfied initially as the pre-condition [26]. Vulnerabilities are illustrated by ovals with white or light blue colors representing the known or zero-day vulnerabilities, respectively. Zero-day vulnerabilities are a subset of documented vulnerabilities over the reporting period. They are vulnerabilities that have been exploited by attackers before corresponding patches are released. The component in the networks is affected before the vulnerabilities in the component are found [27]. By exploiting the zero-day vulnerabilities, severe effects will be brought to the wind farm SCADA/EMS network. Without prior knowledge of the zero-day vulnerabilities, the faults resulted from software flaws are less predictable. Also, since existing metrics for known vulnerabilities are inefficient to an unknown vulnerability, it is difficult to measure the potential impact of the zero-day vulnerabilities [28].

One vulnerability can be exploited when its S_i, N_i, and L_i are satisfied. In Fig. 7, privilege $user(0)$ represents the host of the attacker, it should exist and be connected to the

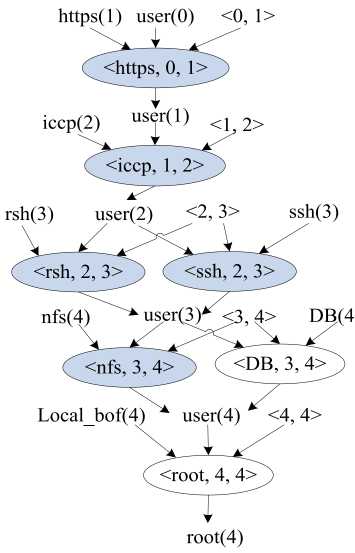

Fig. 7. Bayesian attack graph models of the wind farm control center LAN.

web server, which is shown by $user(1)$. Also, the connection $< 0,1 >$ between the intruder and the web server should be satisfied. $https(1)$ is the Hyper Text Transfer Protocol (HTTP) over Secure Socket Layer (SSL) service executed on the web server, it should be available if the intruder for the unauthorized access to the web server. The user privilege of the web server is obtained when the exploit $\langle https, 0, 1\rangle$ of the https service is executed. In the next step, $\langle iccp, 1, 2\rangle$ represents the vulnerability in the ICCP server. In order to exploit vulnerabilities in the ICCP server, the intruder should gain the user privilege $user(1)$. At the same time, the service $iccp(2)$ and the connection between the web server and the ICCP server $< 1,2 >$ should be satisfied. By exploiting vulnerability $< iccp, 1, 2 >$, the intruder is able to obtain the user privilege $user(2)$ of the ICCP server. In order to reach the application server, the attacker can either exploit the vulnerability $< rsh, 2, 3 >$ or $< ssh, 2, 3 >$, which are vulnerabilities in the remote shell (rsh) service, or Secure Shell (SSH) service found on the application server. Then the user privilege of the operator console (i.e., (4)) can be gained if one of vulnerabilities in $< nfs, 3, 4 >$ or $< DB, 3, 4 >$ are exploited. $nfs(4)$ and $DB(4)$ indicate the Network File System (NFS) service and the Database (DB) service, respectively. Finally, the root privilege of the operator console, which is represented as $root(4)$, can be obtained by the attacker if the buffer overflow is caused at $user(4)$.

Fig. 8 illustrates the Bayesian attack graph model of the communication link between two networks or components of the wind farm SCADA/EMS system. The model is composed of three layers. The first layer represents countermeasures CM_i against attacks. The second layer is denoted by sub-goals SG_i. By bypassing or defeating corresponding countermeasures CM_i, the sub-goals are to be reached. The third layer is composed of the overall goals. One overall goal OG_i can be achieved by reaching the connected sub-goals SG_i.

Three steps are necessary to calculate the probabilities that attacker is able to successfully reach the goal condition. The first step is the estimation of probability that an attacker is able to execute each exploit independently. In the second step, the pre-conditions of the vulnerability are calculated. In the third step, each probability of the successful exploit resulting in its goal condition is calculated. Since different exploits between two conditions can be selected by the attacker, the ratios of the exploit selections are calculated with the backward traversal approach. The detailed approach to determining the probability that the attacker successfully reaches the goal condition is discussed in [11].

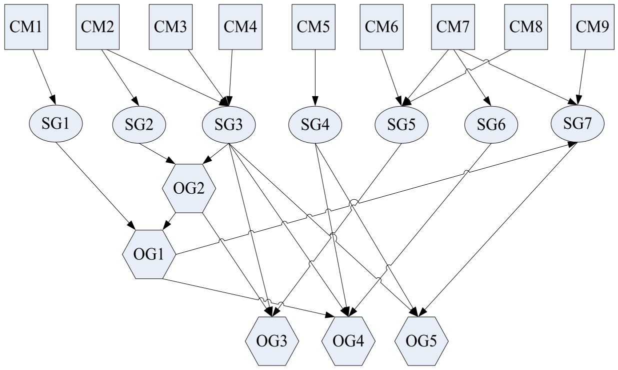

Fig. 8. Bayesian attack graph model of the communication links.

B. MTTC Model of Cyber Attacks

By considering various skill levels of the attackers, the modified MTTC model [11] is applied to estimate the time interval that one vulnerability can be exploited by attackers. The skill level of an attacker indicates the ratio of exploitable vulnerabilities. Four levels of attackers are assumed, which are novice, beginner, intermediate, and expert [29], and the ratio of the successful vulnerability exploit will increase when the skill level is higher.

The procedures of intruders are divided into three statistical processes. Process 1 illustrates that the attacker has found one or several exploits to the identified vulnerabilities. The process 2 is mutually exclusive to the process 1, which means no exploits are found by the attacker, but one or several vulnerabilities are identified. Process 3 illustrates neither vulnerabilities nor exploits are available to the attacker. Process 3 is parallel to processes 1 and 2.

The overall compromise time T of one exploit is estimated by considering the time consumed by all three processes:

$$T = t_1 P_1 + t_2 (1 - P_1) (1 - u) + t_3 u(1 - P_1) \qquad (1)$$

where t_1 is the expected time in process 1, and P_1 is the probability that the attacker is in process 1. t_2 represents the average time in process 2, u indicates the probability of the unsuccessful process 2. t_3 is the expected time of process 3.

With the attack graph and the overall time of each exploit, the MTTCs of the goal conditions in various networks or links are calculated. The MTTC of a goal condition is the sum of portioned overall time of each exploit leading to its post-condition.

Given the attack graph $G(V \bigcup C)$ and one goal condition c, the MTTC of this goal condition is:

$$MTTC\,(c) = \frac{\sum_{v_i \in V} T(v_i) \cdot p(v_i \wedge c)}{p(c)} \tag{2}$$

where $T(v_i)$ is the overall time needed to exploit the vulnerability v_i. $p(v_i \wedge c)$ represents the probability of the successful vulnerability which leads to the goal condition, and $p(c)$ represents the probability that the goal condition is successfully reached.

The MTTC to the target component is the sum of all MTTCs of goal conditions, which is represented as:

$$MTTC = \sum_{j=1}^{n} MTTC(c_j) \tag{3}$$

It should be noticed that zero-day vulnerabilities impact models of the probability that attackers are able to successfully reach the goal condition, as well as the MTTC models. In the first step of the Bayesian attack graph modeling, the dependent probability of the successful exploit on a zero-day vulnerability is assumed as 0.08, whereas the dependent probability of the exploit on a known vulnerability is between 0 and 1. Also, in the MTTC model, more average time is needed for discovering and creating the zero-day vulnerability, thus the MTTC on exploiting one zero-day is larger than the MTTC on exploiting the known vulnerability exploit. More detailed discussions can be found in [11].

V. Wind Farms and Power System Reliability Analysis

A. Wind Power Modeling

The wind speed needs to be forecasted in a reasonably accurate fashion in the reliability assessment of a power system containing wind farms. The wind speed in a wind farm is time-varying and is associated with the wind speeds in the previous hours. There are a number of wind forecasting methods which can be used in power system reliability assessment. In this study, the autoregressive moving average (ARMA) [20] model is adopted. The general ARMA model with m autoregressive terms and n moving average terms is denoted as ARMA (m, n), which is shown as follows:

$$\begin{aligned} y_t = \emptyset_1 \times y_{t-1} + \emptyset_2 \times y_{t-2} + \cdots + \emptyset_m \times y_{t-m} + \alpha_t - \theta_1 \\ \times \alpha_{t-1} - \theta_2 \times \alpha_{t-2} - \cdots - \theta_m \times \alpha_{t-n} \end{aligned} \tag{4}$$

where y_t represents the value of the time-series at time t; $\emptyset_i (i = 1, 2, \cdots, m)$ are the autoregressive parameters; $\theta_j (j = 1, 2, \cdots, n)$ are the moving average parameters; and α_t is a normal white noise time-series denoted by $\alpha_t \in (0, \sigma_a^2)$ and σ_a^2 is the variance.

The simulated hourly wind speed SW_t can be obtained as follows [20]:

$$SW_t = \mu_t + \sigma_t \times y_t \tag{5}$$

where μ_t is the mean value of the observed wind speeds at hour t and σ_t is its standard deviation.

The power output of a wind turbine generator $P_w(SW_t)$ can be calculated using the nonlinear function relationship [30] between the wind turbine output and the wind speed as shown below:

$$\begin{aligned} & P_w(SW_t) \\ & \quad = \begin{cases} 0 & 0 \leq SW_t < V_{ci} \\ (\tau_1 + \tau_2 \times SW_t + \tau_3 \times SW_t^2) P_r & V_{ci} \leq SW_t < V_r \\ P_r & V_r \leq SW_t < V_{co} \\ 0 & SW_t \geq V_{co} \end{cases} \end{aligned} \tag{6}$$

where V_{ci}, V_r and V_{co} are the cut-in speed, rated speed, and cut-out speed, respectively; and τ_1, τ_2 and τ_3 are constants associated with the speeds V_{ci}, V_r and V_{co} [30].

B. Attack Strategy Modeling

Wind turbines in a wind farm are controlled by multiple cyber control systems at different levels, such as WTCP, wind farm local control LAN, and the control center LAN. If one control system is targeted and compromised, the attacker could gain the privilege to disconnect the wind turbines associated with that control system. The time required for compromising the control system is described by the time-to-compromise t_c. Its mean value is modeled by MTTC in section IV, and it refers to the expected time required for the attacker to gain the desired control privilege. The reasonable and intelligent attacker will not send fabricated commands to trip the wind turbines immediately after he gains the privilege, as there might be no wind at that moment. The attacker may remain undetected and wait for the optimal moment to launch the attack. However, when the security countermeasures are upgraded, the attacker may be detected or isolated after a limited time interval. For instance, if the password is updated before the vulnerable device is accessed, the attacker will lose the privilege of the device and need to restart the intrusion process. As the intrusion is detected by the IDS, the power system operator will take effective countermeasures to isolate the attacker. Therefore, in this study, the allowed hidden time is assumed to describe the maximal time the attacker can remain hidden even if no attack occurs. The allowed hidden time represents the capability to detect the intrusion of the power system. If an attack is launched during the allowed hidden time, the attacked wind turbine will be in the failure status for a certain time interval. The wind turbine failure time due to the attack is represented by the time-to-repair t_r and its mean value is denoted as mean time-to-repair (MTTR). The time-to-repair mainly refers to the time needed for computer forensics and device restart. And in this time interval the intrusion will be detected and the privilege of the attacker will be degraded with various methods, such as changing the passwords or limiting the access.

The time-to-compromise, allowed hidden time and time-to-repair are illustrated in Fig. 9.

When the attack is prepared against the wind farms during the allowed hidden time, the wind farm is unlikely to be tripped if there is no wind or the load level is low. It is reasonable for the attacker to attack the wind farms when the conventional generation is low, the load demand is high and

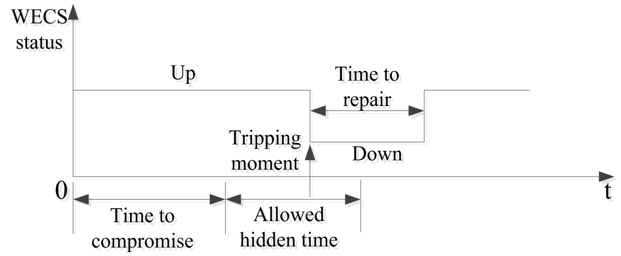

Fig. 9. Attack strategy illustration

the wind is strong. Considering these, an attack strategy is developed based on $V_a\,(t)$.

$$V_a\,(t) = P_{gen}\,(t) - P_{load}\,(t) - \Delta P_{attack}(t) \tag{7}$$

where $V_a\,(t)$ is an index to measure the system state security; $P_{gen}\,(t)$ is the total conventional generation capacity at time t; $P_{load}\,(t)$ is the total load demand at time t; and $\Delta P_{attack}(t)$ is the wind power that can be tripped by the attacker. $\Delta P_{attack}(t)$ varies with time and depends on the privilege of the attacker. If the attacker gains the privilege to control one wind turbine, $\Delta P_{attack}(t)$ equals $P_w(SW_t)$; if the attacker can control the whole wind farm, $\Delta P_{attack}(t)$ can be calculated as follows:

$$\Delta P_{attack}\,(t) = P_w(SW_t) \times n_{turbine} \tag{8}$$

where $n_{turbine}$ is the number of wind turbines in the attacked wind farm.

The attacker estimates the system state and calculates $V_a\,(t)$ during the allowed hidden time. An attack will be performed when $V_a\,(t)$ is minimal, which is the tripping moment shown in Fig. 9. It is noted that some highly intelligent attackers could develop more sophisticated methods to determine the tripping moment, which is beyond the scope of this paper.

The estimation of the tripping moment based on (7) and (8) is essentially a minimization problem, which requires the attacker to accurately predict the total conventional generation capability, the wind generation and the load demands during the hidden time. Generally, the number of conventional generators, the up/down status, and the generation capability of each generator are fixed during the short hidden time, and this information can be obtained by the attacker through cyber sniffing, social engineering, or even some public data. After obtaining the necessary information, the conventional generation capability can be readily known. And some methods have been developed for predicting the load demand and wind power generation. The load demand profile usually follows a chronological pattern due to the related human activity pattern. Intelligent attackers can reasonably predict the short-term load demand if they are able to intercept the current and historical load demand data. And the prediction can be made through different methods, such as wavelet neural network in [31] and functional time-series method in [32]. The wind power forecast can be conducted based on multiple methods to achieve an acceptable accuracy. For instance, attackers may use the probabilistic hybrid approach in [33], or ARMA in [34]. As generation and load forecasting is critical to power system scheduling and operation, it is believed that more advanced methods will be developed in the future research of this area.

Even though the accuracy of the wind prediction has been significantly increased by various forecasting methods, it is a challenging task for the attackers to perfectly predict generations and load demands due to inevitable uncertainties in the load demand and renewable generation. Also, the attacker may have difficulties in obtaining the necessary data for performing the prediction. Therefore, considering the inherent inaccuracy of the prediction methods and the uncertain behavior of the attackers, it is not guaranteed that the attacker is always able to make the exact prediction and obtain the optimal tripping moment described by (7) and (8). However, it is crucial for the defender to be aware of the optimal tripping moment so that countermeasures against the attacks could be enforced and improved. And in this paper, a conservative assessment of the security is performed by assuming that the attackers can obtain the absolute minimum $V_a\,(t)$ in the power system adequacy evaluation.

C. Reliability Evaluation Procedures

For a bulk power system, several wind farms can be integrated and connected to different buses. In order to attack the wind turbines, all control systems related to the wind turbines could be chosen as attack targets by the attackers. Inspired by the power system reliability assessment procedure in [35], an integrated power system evaluation framework considering the cyber attacks against the wind farms is proposed based on sequential Monte Carlo simulation as depicted in Fig. 10, which is detailed as follows:

(1) Model the reliability of major physical components in the power system, mainly including the conventional generators and transmission lines. Generate a time sequence representing the working status of each element.

(2) Model the wind speeds in each wind farm. This is described by the ARMA model in Part A of Section V. Generate a time sequence representing the working status of each wind turbine.

(3) Generate an annual chronological curve for the load at each bus.

(4) Randomly sample a t_c for the selected target using $t_c = -In(1-U) \times MTTC$, where U is a random number within [0, 1].

(5) Calculate $V_a\,(t)$ for each hour in the allowed hidden time and determine the tripping moment.

(6) Randomly sample a t_r for the selected target using $t_r = -In(1-U) \times MTTR$.

(7) Check if the sampling time is sufficient. If not, return to step 4 or go to next step.

(8) Check if all the attack targets are sampled. If not, return to step 4 or go to next step.

(9) Update the wind power output of each wind turbine based on the sampling of steps 4-8.

(10) Sequentially sample the composite system state at time t. A composite system state includes the load demands, transmission line statuses, conventional generator statuses and

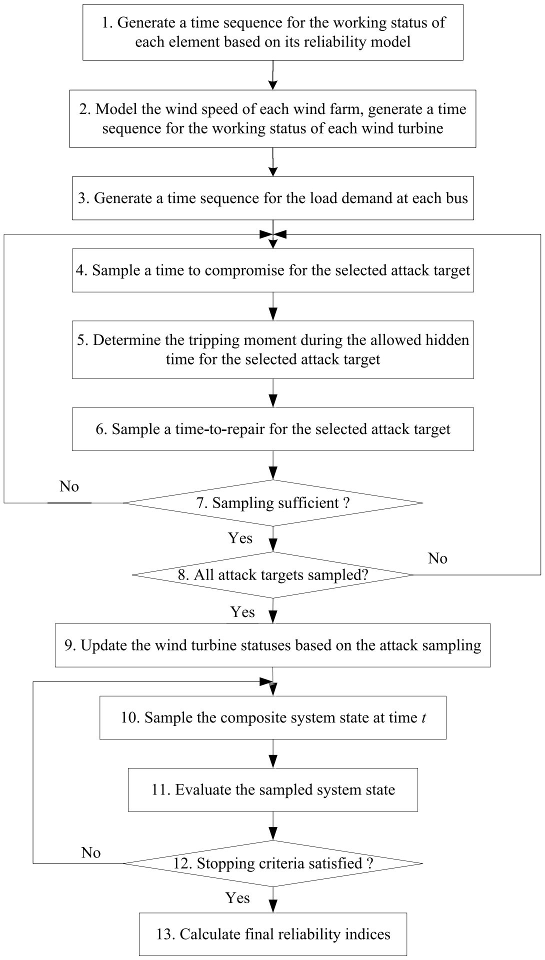
1. Generate a time sequence for the working status of each element based on its reliability model
2. Model the wind speed of each wind farm, generate a time sequence for the working status of each wind turbine
3. Generate a time sequence for the load demand at each bus
4. Sample a time to compromise for the selected attack target
5. Determine the tripping moment during the allowed hidden time for the selected attack target
6. Sample a time-to-repair for the selected attack target
No
7. Sampling sufficient ?
Yes
No
8. All attack targets sampled?
Yes
9. Update the wind turbine statuses based on the attack sampling
10. Sample the composite system state at time t
11. Evaluate the sampled system state
No
12. Stopping criteria satisfied ?
Yes
13. Calculate final reliability indices

Fig. 10. Integrated power system reliability assessment considering cyber attacks against wind generations.

wind turbine power outputs.

(11) Evaluate the sampled composite power system state. This is accomplished by performing the DC optimal power flow analysis.

(12) Check if the stopping criteria are met or not. If not, go back to step 10. The state sampling is conducted for 100 years.

(13) Calculate the desired reliability indices. In this study, the indices evaluated are the expected energy not supplied (EENS) and loss of load probability (LOLP).

VI. Simulation Results and Analysis

A. Bayesian Attack Graphs and MTTCs of Targets

In order to simplify the attack graphs, nodes which represent privilege (L) and exploits to vulnerabilities V remain, and the nodes service (S) and connection (N) are omitted. In each simplified attack graph, different numbers of known and zero-day vulnerabilities are assumed in each component. The type of vulnerabilities is assumed by the possible service executed on the component. For instance, HTTPS is one possible service executed on the web server in the wind control center. The number of the zero-day vulnerabilities is assumed by the complexity and the security mechanism of the cyber network.

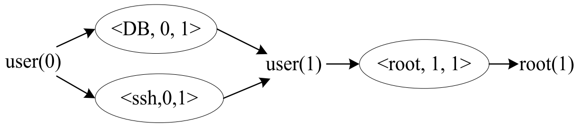

Fig. 11. Attack graph model to compromise the WTCP.

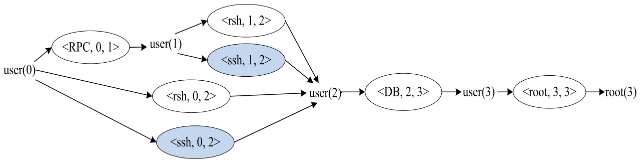

Fig. 12. Attack graph model to compromise the local control LAN.

When more advanced security mechanism is adopted on the crucial network, less known vulnerabilities will be available to cyber intruders. In order to reach the targeted component in the network, zero-day exploits should be created by the attacker and more average time is needed for the successful intrusion.

The Bayesian attack graph of the WTCP is illustrated in Fig. 11. The attack path between the intruder ($user(0)$) and the target ($root(1)$) shows the processes to gain the root privilege of the WTCP. Since the attacker may directly reach the WTCP, it is assumed the user privilege can be gained by bypassing one firewall and executing two exploits of the vulnerabilities on the targeted WTCP. It is assumed that the executed exploits in the target are two known vulnerability exploits $< ssh, 0, 1 >$ and $< DB, 0, 1 >$. And the attacker will obtain the root privilege by exploiting the known root vulnerability $< root, 1, 1 >$.

The attack graph of the local control LAN for one wind farm is illustrated in Fig. 12. Based on the network configuration, it is assumed that the communication server and the application server can be reached by the attacker. One known vulnerability $< RPC, 0, 1 >$ is assumed in the communication server. The attacker may first breach the communication server and obtain the user privilege, and he will exploit two vulnerabilities in the application server, which are one known vulnerability $< rsh, 1, 2 >$, and one zero-day vulnerability $< ssh, 1, 2 >$ in light blue color, and gain the user privilege of the application server. He can also directly gain the user privilege of the application server by executing the exploits $< ssh, 0, 2 >$ and $< rsh, 0, 2 >$. Then the attacker will reach the targeted wind farm workstation by executing the exploit $< DB, 2, 3 >$ and $< root, 3, 3 >$.

Fig. 13 represents the attack graph of the backup remote control LAN. Since the ICCP server is the only component which communicates with the outside network, the intruder should first attack the ICCP server. It is assumed that when one zero-day vulnerability $< iccp, 0, 1 >$ is exploited in the ICCP server. The next cyber component is the application server, it has two vulnerabilities to exploit, which are the known vulnerability $< rsh, 1, 2 >$ and the zero-day vulnerability $< ssh, 1, 2 >$. And the operator console can be controlled when the zero-day vulnerability $< nfs, 2, 3 >$ and the root

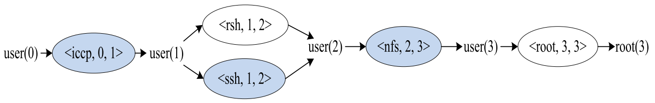

Fig. 13. Attack graph model to compromise the remote control LAN.

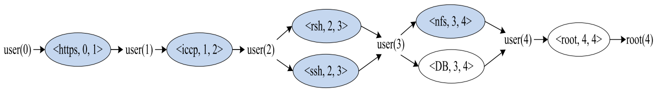

Fig. 14. Attack graph model to compromise the control center LAN.

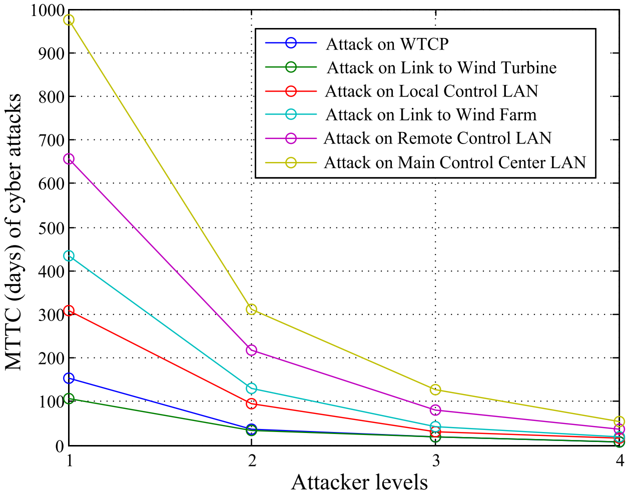

Fig. 15. MTTC of cyber attacks on the wind farm SCADA/EMS.

TABLE I
MTTRS RELATED TO CYBER ATTACK TARGETS

Targets	MTTR (h)
WTCP	10
Link to WTCP	10
Local Control LAN	20
Link to Wind Farm	20
Remote Control LAN	50
Control Center LAN	50

vulnerability are exploited.

Fig. 14 illustrates the attack graph of the control center LAN, which has the largest number of vulnerabilities to be exploited. It is assumed that one zero-day vulnerability $< https, 0, 1 >$ is found in the web server, and one zero-day vulnerability $< iccp, 1, 2 >$ is exploited in the ICCP server. $< rsh, 2, 3 >$ and $< ssh, 2, 3 >$ in the application server are exploited as zero-day vulnerabilities. The user privilege of the control center operator console can be gained by exploiting one known vulnerability $< DB, 3, 4 >$ and one zero-day vulnerability $< nfs, 3, 4 >$, and the root privileges of the operator console can be obtained by exploiting the vulnerability $< root, 4, 4 >$.

On the communication links, one target is the link between the WTCP and the wind turbine, and the other is the link between the control center LAN and the local control LAN. Since the first link can be found beside the WTCP, which is not difficult to reach, it is assumed all vulnerabilities of the link are known vulnerabilities. The link connected to the wind farm may be equipped with several countermeasures, such as encryption and physical protection. This will bring additional difficulty to attackers, thus vulnerabilities in the link connected to the wind farms are assumed as zero-day ones.

As the attack levels are novice, beginner, intermediate, and expert, the fractions of the vulnerabilities that are exploitable are assumed as 0.2, 0.4, 0.6, and 0.8. And the MTTCs of gaining the control privileges on different targets in the wind farm SCADA/EMS system are shown in Fig. 15. It can be observed that as the skill levels of intruders increase, less MTTC is needed for the successful intrusion. For the novice, the MTTCs are between 105.3193 and 975.6548 days. The beginner needs 32.9701 to 311.4075 days for the successful attacks on the six targets. 17.8272 to 127.7913 days are needed by attacker with the intermediate level, and only 8.3194 to 52.6561 days are needed by the expert for the successful attacks. For the simplest WTCP network, MTTC of the novice attacker is about 152 days, whereas the attacker with the expert level needs only about 8 days.

It is also found that when more zero-day vulnerabilities are exploited in the network, larger MTTC is needed to gain the root privilege of the target component. With the same skill level, more MTTC is needed for the successful attack on the control center, which possesses the most complicated and secure cyber network. Compared with the control center, the network of the WTCP is the least complicated one, which has only one firewall as the countermeasure. As all vulnerabilities are assumed to be the known ones, the least MTTC is needed for the successful attack on the WTCP.

B. Power System Reliability Evaluation Results

For the wind power modeling, wind turbines with a rated power of 1.5 MW, and cut-in, rated and cut-out speeds of 4, 11.1 and 20 m/s, respectively are used in this study. The physical failures of the wind turbines are not considered here due to their relatively minor effect and the focal point of this work. And the wind speed data of stations 9,366 and 1,732 from year 2004 to 2006 in [36] are analyzed and simulated by the ARMA (3, 2) model. The average value of the simulated wind speed is 9.0 m/s and 8.7 m/s for station 9366 and station 1732, respectively.

In this study, the simulations are conducted based on modified IEEE RTS79 systems [37]. The IEEE RTS79 system has 24 buses, 32 generating units and 38 branches.

The attackers can attack different cyber targets and the MTTCs are estimated as shown in Fig. 15, and the related MTTRs are assumed in Table I.

In power system reliability evaluation, two common sets of indices are widely applied to model the power system reliability: annualized indices where a single level of load is

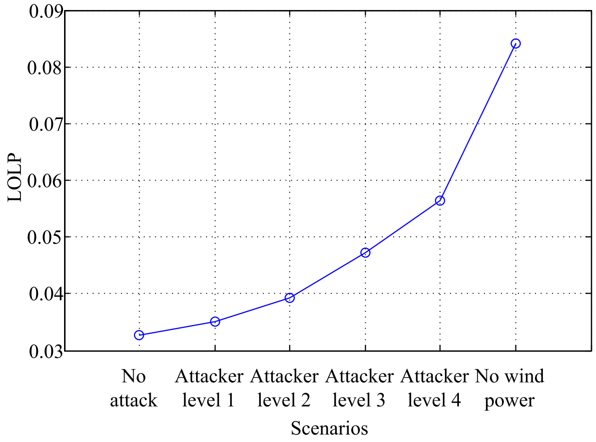

Fig. 16. Annualized LOLP indices for different scenarios

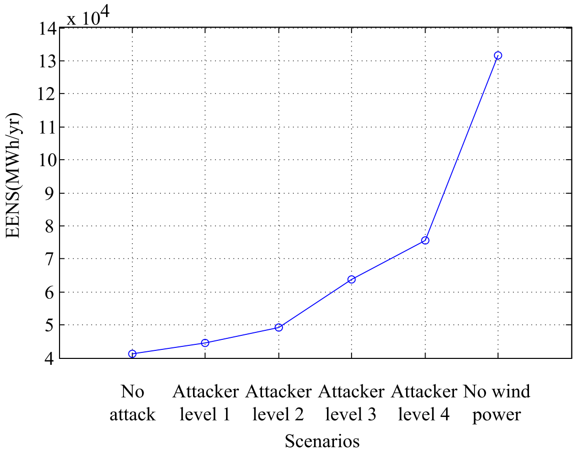

Fig. 17. Annualized EENS indices for different scenarios.

applied; annual index where the time-varying chronological load curve is applied. In our study, these two cases are both considered.

1) Annualized indices: The peak load value of the IEEE RTS79 system is 2,850 MW and it is applied to this study. On bus 22, a wind farm with 200 wind turbines is added and the wind speed in station 9366 is applied. On bus 2, a wind farm with 100 wind turbines is added and the wind speed in station 1732 is applied. In this simulation, six scenarios are studied, and the LOLP and EENS indices are shown in Fig. 16 and Fig. 17, respectively, and the allowed hidden time is assumed as 100 hours. Four levels of attackers are considered, and level 1, level 2, level 3 and level 4 attackers are novice, beginner, intermediate, and expert, respectively. Their MTTCs are calculated as shown in Fig. 15. The scenario “no wind power” means wind power generations are not considered.

When wind power farms are considered and the cyber attacks are ignored as shown in the case of “no attack”, the LOLP value is 0.033 and the EENS value is 41,170 MWh/yr. And this scenario is similar to the case studies in [20]-[22]. When the wind farms are attacked by the level 1 attackers, the LOLP value is increased to 0.035 and the EENS value is increased to 44,423 MWh/yr. This clearly demonstrates that cyber attacks against the wind farms have a non-negligible impact on the overall power system reliability.

When the skill level of the attacker increases, the MTTC will decrease, which indicates the cyber attacks will become more frequent. As shown in Fig. 16 and Fig. 17, the LOLP and EENS indices both increase due to the increased frequency of cyber attacks. This indicates that the skills and capabilities of the attackers are important factors for influencing the power system reliability.

2) Annual indices: The annual indices consider the chronological change of the load demands, and thus it can better reflect the practical power system reliability while the calculation of the annual indices requires more computational time than the annualized indices.

The simulation is conducted based on the IEEE RTS79 system and the system is modified to better demonstrate our ideas. On bus 22, the original six 50 MW generating units are removed and a wind farm with 200 wind turbines is added, and the wind speed in station 9366 is adopted. On bus 2, the original two 76 MW generators are removed and a wind farm with 100 wind turbines is added, and the wind speed in station 1732 is adopted.

The simulation results are shown in Fig. 18 and Fig. 19. In the case study of “no attack”, the LOLP value and the EENS value are 0.0074 and 10,200 MWh/yr, respectively. Further, the LOLP and EENS increase with the decrease of MTTC. For example, when the wind farms are attacked by level 1 attackers, the LOLP value and EENS values are increased to 0.0082 and 11,133 MWh/yr respectively when the allowed hidden time is 100 hours. And this proves the negative impact of cyber attacks against wind farms on the reliability of the power system.

In both Fig. 18 and Fig. 19, the LOLP and EENS values increase when the levels of attackers are increased. It implies that if the higher level attacker can compromise the targeted cyber network within a shorter intrusion time, the power system reliability will decrease due to the increased occurrence of cyber attacks.

In order to demonstrate the influence of the allowed hidden time, comparisons are made when the allowed hidden times are 1 hour and 100 hours, respectively. It is shown that the LOLP and EENS indices have larger values when more allowed hidden time is given. Since the allowed hidden time can reflect the defense level of the system, the simulation result indicates that the improvement of the cyber detection capability and frequent updates of patches for the system are beneficial to maintaining the power system reliability.

In summary, the annualized indices and annual indices verify that cyber attacks against wind generation can affect the power system reliability, and the power system reliability increases with the increase of the MTTC and the decrease of the allowed hidden time. These conclusions advocate the necessity and urgency of taking effective actions to enhance the cybersecurity of modern power grids.

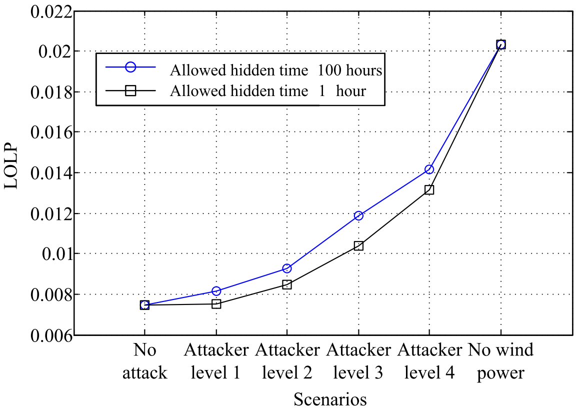

Fig. 18. Annual LOLP indices for different scenarios.

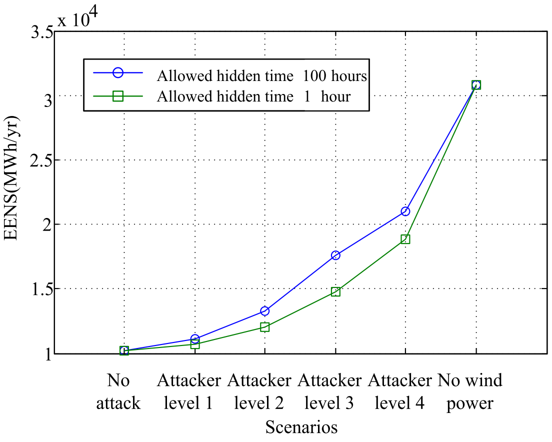

Fig. 19. Annual EENS indices for different scenarios.

VII. Conclusion and Future Work

In this paper, the cyber attack scenarios on the wind farm SCADA/EMS system are discussed with the Bayesian attack graph models. MTTCs of successful attacks against the wind farm SCADA/EMS are evaluated based on various cyber attack paths and skill levels of attackers. It is illustrated that a larger MTTC is needed when more unknown vulnerabilities are exploited. Also, a less attack time interval is needed for attackers with higher skill levels. The reliability of the power system considering various cyber attacks against the wind farms is evaluated based on the IEEE RTS79 system. The reliability indices including LOLP and EENS are derived accordingly. It is found that the power system becomes less reliable when more wind turbines are tripped and less MTTCs are consumed. Also, advanced cyber intrusion detection techniques can help to maintain the power system reliability. This study can be a starting point for quantitative security analysis in wind integrated power system reliability evaluation, and may provide some useful insights for enabling informed decision-making associated with cybersecurity budget allocation.

In the future research, more cyber attack scenarios in the wind farm SCADA/EMS system will be examined and analyzed. Countermeasures of the wind farm networks will be considered with the Bayesian and MTTC models. Different renewable energies affecting the power system reliability will be investigated with the cyber attacks, and their impacts on the overall system reliability will be evaluated.

References

[1] American Wind Energy Association: American wind power reaches major power generation milestones in 2013. [Online]. Available: http://www.awea.org/MediaCenter/pressrelease.aspx?ItemNumber=6184

[2] U.S. Department of Energy: 20% Wind Energy by 2030. [Online]. Available: http://www.nrel.gov/docs/fy08osti/41869.pdf

[3] F. Yu, P. Zhang, W. Xiao, and P. Choudhury, “Communication systems for grid integration of renewable energy resources,” *IEEE Netw.*, vol. 25, no. 5, pp. 22–29, Sep. 2011.

[4] J. Yan, C.-C. Liu, and M. Govindarasu, “Cyber intrusion of wind farm SCADA system and its impact analysis,” in *2011 IEEE PES Power Systems Conference and Exposition*, 2011, pp. 1–6.

[5] G. J. Smith, “SCADA in wind farms,” in *Instrumentation in the Electrical Supply Industry, IEE Colloquium*, pp. 11/1–11/2, Jun. 1993.

[6] D. R. Edmunds, “Green Energy Leaves National Grid More Vulnerable to ‘Constant’ Cyber-Attacks,” http://www.breitbart.com/london/2015/01/12/green-energy-leaves-national-grid-more-vulnerable-to-constant-cyber-attacks/, Jan. 12, 2015.

[7] S. Karnouskos, “Stuxnet worm impact on industrial cyber-physical system security,” in *IECON 2011 - 37th Annual Conference of the IEEE Industrial Electronics Society*, 2011, pp. 4490–4494.

[8] L. Wang, S. Jajodia, A. Singhal, P. Cheng, and S. Noel, “k-Zero Day Safety: A Network Security Metric for Measuring the Risk of Unknown Vulnerabilities,” *IEEE Trans. Dependable Secur. Comput.*, vol. 11, no. 1, pp. 30–44, Jan. 2014.

[9] S. Sridhar and G. Manimaran, “Data integrity attacks and their impacts on SCADA control system,” in *IEEE PES General Meeting*, 2010, pp. 1–6.

[10] S. Sridhar, A. Hahn, and M. Govindarasu, “Cyber attack-resilient control for smart grid,” in *2012 IEEE PES Innovative Smart Grid Technologies (ISGT)*, 2012, pp. 1–3.

[11] Y. Zhang, L. Wang, Y. Xiang, and C.-W. Ten, “Power System Reliability Evaluation With SCADA Cybersecurity Considerations,” *IEEE Trans. Smart Grid*, vol. 6, no. 4, pp. 1707 - 1721, 2015.

[12] J. Yan, M. Govindarasu, C.-C. Liu, and U. Vaidya, “A PMU-based risk assessment framework for power control systems,” in *2013 IEEE Power & Energy Society General Meeting*, 2013, pp. 1–5.

[13] B. Chen, N. Pattanaik, A. Goulart, K. L. Butler-purry, and D. Kundur, “Implementing attacks for modbus/TCP protocol in a real-time cyber physical system test bed,” in *2015 IEEE International Workshop Technical Committee on Communications Quality and Reliability (CQR)*, 2015, pp. 1–6.

[14] A. Stefanov and C.-C. Liu, “ICT modeling for integrated simulation of cyber-physical power systems,” in *2012 3rd IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe)*, 2012, pp. 1–8

[15] M. Wei and Z. Chen, “Study of LANs access technologies in wind power system,” in *IEEE PES General Meeting*, 2010, pp. 1–6.

[16] B. R. Karthikeya and R. J. Schutt, “Overview of Wind Park Control Strategies,” *IEEE Trans. Sustain. Energy*, vol. 5, no. 2, pp. 416–422, Apr. 2014.

[17] L. Xie and M. D. Ilic, “A module-based approach to integrating wind power for guaranteed power system stability,” in *2008 First International Conference on Infrastructure Systems and Services: Building Networks for a Brighter Future (INFRA)*, 2008, pp. 1–6.

[18] K. Gajrani, A. Bhargava, K. G. Sharma, and R. Bansal, “Cyber security solution for wide area measurement systems in wind connected electric grid,” in *2013 IEEE Innovative Smart Grid Technologies-Asia (ISGT Asia)*, 2013, pp. 1–5.

[19] L. Wang, H. Li, Z. Chen, and H. Xu, “Vulnerable branch assessment of power grid contains double-fed wind farms,” in *2014 International Conference on Power System Technology*, 2014, pp. 2727–2733.

[20] R. Billinton and G. Bai, “Generating Capacity Adequacy Associated With Wind Energy,” *IEEE Trans. Energy Convers.*, vol. 19, no. 3, pp. 641–646, Sep. 2004.

[21] L. Wang and C. Singh, “Population-Based Intelligent Search in Reliability Evaluation of Generation Systems with Wind Power Penetration,” *IEEE Trans. Power Systems*, vol. 23, no. 3, pp. 1336–1345, Aug. 2008.

[22] R. Billinton, R. Karki, Y. Gao, D. Huang, P. Hu and W. Wangdee, "Adequacy Assessment Considerations in Wind Integrated Power Systems," *IEEE Trans. Power Systems*, vol. 27, no. 4, pp. 2297 - 2305, July 2012.

[23] J.-M. Gallardo-Calles, A. Colmenar-Santos, J. Ontañon-Ruiz, and M. Castro-Gil, "Wind control centres: State of the art," *Renew. Energy*, vol. 51, pp. 93–100, Mar. 2013.

[24] L. E. Arnold and J. Hajagos, "LIPA implementation of real-time stability monitoring in a CIM compliant environment," in *2009 IEEE PES Power Systems Conference and Exposition*, 2009, pp. 1–6.

[25] J. Verba and M. Milvich, "Idaho National Laboratory Supervisory Control and Data Acquisition Intrusion Detection System (SCADA IDS)," in *2008 IEEE Conference on Technologies for Homeland Security*, 2008, pp. 469–473.

[26] W. Nzoukou, L. Wang, S. Jajodia, and A. Singhal, "A Unified Framework for Measuring a Network's Mean Time-to-Compromise," in *2013 IEEE 32nd International Symposium on Reliable Distributed Systems*, 2013, pp. 215–224.

[27] "2015 Internet Security Threat Report", Symantec, Volume 20, April, 2015, [Online]. Available: https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347931_GA-internet-security-threat-report-volume-20-2015-appendices.pdf.

[28] L. Wang, S. Jajodia, A. Singhal, and S. Noel, "k-zero day safety: measuring the security risk of networks against unknown attacks," pp. 573–587, Sep. 2010.

[29] M. A. McQueen, W. F. Boyer, M. A. Flynn, and G. A. Beitel, "Time-to-compromise model for cyber risk reduction estimation," *First Workshop on Quality of Protection*, Milan, Italy, September 15, 2005.

[30] P. Giorsetto and K. F. Utsurogi, "Development of a new procedure for reliability modeling of wind turbine generators," *IEEE Trans. Power App. Syst.*, vol. PAS-102, pp. 134–143, 1983.

[31] P. B. Luh, L. D. Michel, M. A. Coolbeth, P. B. Friedland, and S. J. Rourke, "Short-Term Load Forecasting: Similar Day-Based Wavelet Neural Networks," *IEEE Trans. Power Syst.*, vol. 25, no. 1, pp. 322–330, Feb. 2010.

[32] E. Paparoditis and T. Sapatinas, "Short-Term Load Forecasting: The Similar Shape Functional Time-Series Predictor," *IEEE Trans. Power Syst.*, vol. 28, no. 4, pp. 3818–3825, Nov. 2013.

[33] A. U. Haque, M. H. Nehrir, and P. Mandal, "A Hybrid Intelligent Model for Deterministic and Quantile Regression Approach for Probabilistic Wind Power Forecasting," *IEEE Trans. Power Syst.*, vol. 29, no. 4, pp. 1663–1672, Jul. 2014.

[34] R. Billinton and R. Ghajar, "A sequential simulation technique for adequacy evaluation of generating systems including wind energy," *IEEE Trans. Energy Convers.*, vol. 11, no. 4, pp. 728–734, 1996.

[35] R. Billinton and W. Li, *Reliability Assessment of Electric Power Systems Using Monte Carlo Methods*, New York; London: Plenum, 1994.

[36] NREL, Western Wind Resources Dataset. [Online]. Available: http://wind.nrel.gov/Web_nrel/.

[37] P. M. Subcommittee, "IEEE reliability test system," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-98, no. 6, pp. 2047-2054, Nov. 1979.

Yichi Zhang (S'10) received the B.E. degree in Electronics Information Engineering from Yanshan University, Qinhuangdao, China, in 2009, the M.S. and Ph.D. degrees in Electrical Engineering from the University of Toledo, Ohio, USA, in 2011 and 2015, respectively. Her major research interests include cybersecurity of smart grid and cyber-physical systems.

Yingmeng Xiang (S'11) received the B.S. degree in electrical engineering from Chongqing University, Chongqing, China in 2010 and the M.S. degree in electrical engineering from Huazhong University of Science and Technology, Wuhan, China in 2013. He is currently working toward the Ph.D. degree in electrical engineering in the Department of Electrical Engineering and Computer Science, University of Wisconsin-Milwaukee, Milwaukee, WI, USA. His research interests include power system adequacy evaluation, cyber-physical system modeling, and power system operations.

Lingfeng Wang (S'02-M'09) received the B.E. degree in measurement and instrumentation from Zhejiang University, Hangzhou, China, in 1997; the M.S. degree in electrical and computer engineering from the National University of Singapore, Singapore, in 2002; and the Ph.D. degree from the Electrical and Computer Engineering Department, Texas A&M University, College Station, TX, USA, in 2008. He is currently an Associate Professor with the Department of Electrical Engineering and Computer Science, University of Wisconsin–Milwaukee, Milwaukee, WI, USA, where he directs the cyber-physical energy systems research group. He was an Assistant Professor with the University of Toledo, Toledo, OH, USA, and an Associate Transmission Planner with the California Independent System Operator, Folsom, CA, USA. His current research interests include power system reliability and resiliency, smart grid cybersecurity, critical infrastructure protection, energy-water nexus, renewable energy integration, intelligent and energy-efficient buildings, electric vehicles integration, microgrid analysis and management, and cyber-physical systems.

Dr. Wang is an Editor of the IEEE TRANSACTIONS ON SMART GRID, IEEE TRANSACTIONS ON POWER SYSTEMS, and IEEE POWER ENGINEERING LETTERS, and serves on the Steering Committee of the IEEE TRANSACTIONS ON CLOUD COMPUTING. He is also an Editorial Board Member for several international journals, including *Sustainable Energy Technologies and Assessments*, and *Intelligent Industrial Systems*. He served as a Co-chair for IEEE SmartGridComm'15 Symposium on Data Management, Grid Analytics, and Dynamic Pricing.