J. Mod. Power Syst. Clean Energy (2015) 3(3):321–331
DOI 10.1007/s40565-015-0145-8

Risk assessment framework for power control systems with PMU-based intrusion response system

Jie YAN, Manimaran GOVINDARASU, Chen-Ching LIU, Ming NI (✉), Umesh VAIDYA

Abstract Cyber threats are serious concerns for power systems. For example, hackers may attack power control systems via interconnected enterprise networks. This paper proposes a risk assessment framework to enhance the resilience of power systems against cyber attacks. The duality element relative fuzzy evaluation method is employed to evaluate identified security vulnerabilities within cyber systems of power systems quantitatively. The attack graph is used to identify possible intrusion scenarios that exploit multiple vulnerabilities. An intrusion response system (IRS) is developed to monitor the impact of intrusion scenarios on power system dynamics in real time. IRS calculates the conditional Lyapunov exponents (CLEs) on line based on the phasor measurement unit data. Power system stability is predicted through the values of CLEs. Control actions based on CLEs will be suggested if power system instability is likely to happen. A generic wind farm control system is used for case study. The effectiveness of IRS is illustrated with the IEEE 39 bus system model.

Keywords Cyber security, Supervisory control and data acquisition (SCADA), Risk assessment, Intrusion response system (IRS), Conditional Lyapunov exponents (CLEs), Phasor measurement unit (PMU), Voltage instability

1 Introduction

Power systems are vulnerable to cyber attacks. Modern IT technologies are heavily used in today's supervisory control and data acquisition (SCADA) systems of industrial control systems including power systems. While IT technologies bring a lot of benefits, many security risks are introduced as well. For example, the connectivity of SCADA systems and enterprise networks improves business visibility and efficiency, but it makes SCADA systems more vulnerable to cyber attacks. According to the 2003～2006 data from Eric Byres, BCIT, 49 % cyber attacks at industrial control systems are launched via connected enterprise networks. One highly publicized example is Stuxnet, which attacked an industrial control system by infecting those organization networks that interact with the target [1].

In 2006, US Department of Energy (DOE) published "Roadmap to secure control systems in the energy sector" (updated in 2011) [2]. It envisions that: in 10 years, control systems for critical applications will be designed, installed, operated, and maintained to survive an intentional cyber assault with no loss of any critical function. Much effort

CrossCheck date: 29 January 2015

Received: 17 April 2014 / Accepted: 29 January 2015 / Published online: 13 August 2015

J. YAN, Market Engineering, MISO, Carmel, IN 46032, USA
e-mail: jyan@misoenergy.org
M. GOVINDARASU, U. VAIDYA, Department of Electrical and Computer Engineering, Iowa State University, Ames, IA 50011, USA
M. GOVINDARASU
e-mail: gmani@iastate.edu
U. VAIDYA
e-mail: ugvaidya@iastate.edu
C.-C. LIU, School of Electrical Engineering and Computer Science, Washington State University, Pullman, WA 99165, USA
e-mail: liu@eecs.wsu.edu
M. NI, NARI Technology Co. Ltd., Nanjing 211106, China
(✉) e-mail: mingni2002@hotmail.com
ni-ming@sgepri.sgcc.com.cn

has been made to secure power facilities. The DOE National SCADA Test Bed (NSTB) Program, established in 2003, supports industry and government efforts to enhance cyber security of control systems in the energy sector. The NERC standards CIP-002-4 through CIP-009-4 provide a cyber security framework for the identification and protection of critical cyber assets to support reliable operations of the bulk electric system [3]. The International Electrotechnical Commission Technical Council (IEC TC 57), i.e., power system management and associated information exchange, has advanced the standard communication protocol security in IEC 62351 with stronger encryption and authentication mechanisms [4]. The Hallmark Project by Schweitzer Engineering Laboratories, Inc. presents the secure SCADA communications protocol (SSCP) technology which provides integrity for SCADA messages. United States Computer Emergency Readiness Team (US-CERT) has set up awareness programs about system vulnerabilities to improve control system security [5]. The cyber security audit and attack detection toolkit by Digital Bond, Inc. is developed to identify vulnerable configurations in control system devices and applications. Reference [6] presents a risk assessment methodology that accounts for both physical and cyber security of critical infrastructures. In [7], a SCADA security framework is proposed. System vulnerabilities are assessed quantitatively through an attack tree. The impact of a cyber attack on SCADA systems is studied systematically in [8]. It is evaluated by the resultant loss of load through a power flow computation.

This paper presents a new risk assessment framework for SCADA systems of power grids. Individual vulnerabilities within control systems are evaluated based on the duality element relative fuzzy evaluation method (DERFEM). An attack graph is developed to identify possible intrusion scenarios that exploit multiple security vulnerabilities. An intrusion response system (IRS) based on the phasor measurement unit (PMU) data is proposed to assess the impact of intrusion scenarios on power system dynamics.

The main contribution is IRS, which is an on-line monitoring and control scheme based on PMUs. It monitors the impact of cyber intrusions on power system dynamics in real time. If power system instability, such as voltage instability, is judged to be likely after a cyber attack, IRS will act as a mitigation mechanism to prevent power system instability. Unlike traditional security mechanisms, such as encryption and authentication, which increase the complexity of power systems, and may cost additional time in power system operations, IRS uses a control strategy based on the conditional Lyapunov exponents (CLEs) to enhance the resilience of power systems against cyber attacks.

2 Risk assessment framework

The risk assessment framework is shown in Fig. 1. For SCADA systems of a power system, the procedure starts with identification of the configuration of its cyber system. Vulnerabilities within the cyber system are then identified. Each vulnerability is evaluated quantitatively by DERFEM. An attack graph is built to identify possible intrusion scenarios that exploit multiple vulnerabilities. The probability of occurrence of every intrusion scenario is calculated. Once an intrusion scenario is successfully executed, IRS will monitor its impact on power system dynamics in real time. The impact is characterized by CLEs computed on PMU data. If the values of CLEs are high, it implies that voltage instability is likely to happen, and then control actions based on CLEs will be taken to prevent voltage instability.

2.1 DERFEM

Assume that a cyber system has l identified vulnerabilities: r_1, $r_2 \cdots r_l$. DERFEM is employed to assign each vulnerability a scaled value within [0, 1] which quantitatively characterizes the vulnerable level. The larger the scaled value is, the higher the vulnerable level will be.

DERFEM proceeds as follows.

1) Compare a pair of different vulnerabilities (r_i, r_j) so as to obtain the scaled values $\tau_{r_j}(r_i)$ and $\tau_{r_i}(r_j)$. $\tau_{r_j}(r_i)$ represents the vulnerable level of r_i compared to r_j. Likewise, $\tau_{r_i}(r_j)$ represents the vulnerable level of r_j compared to r_i. $0 \leqslant \tau_{r_j}(r_i) \leqslant 1$; $0 \leqslant \tau_{r_i}(r_j) \leqslant 1$. If $\tau_{r_j}(r_i) > \tau_{r_i}(r_j)$, it implies that the vulnerability r_i has a higher vulnerable level than r_j does. $\tau_{r_j}(r_i)$ and $\tau_{r_i}(r_j)$ are from engineering judgments. This method is valid, because engineering

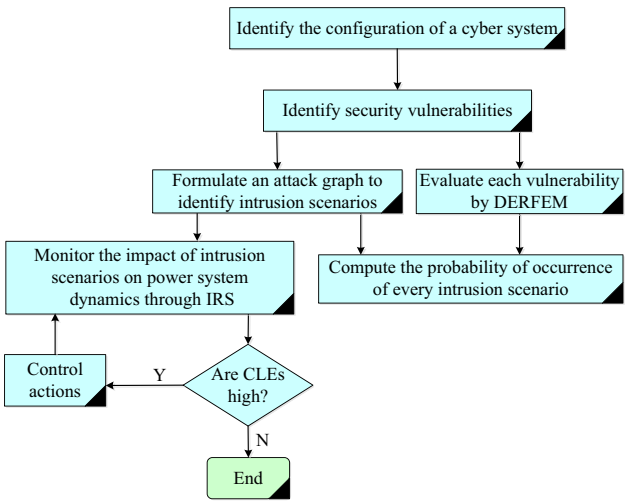

Fig. 1 Proposed risk assessment framework

judgments from different sources are statistically close when it is to compare two vulnerabilities.

2) Continue the comparison of different pairs of individual vulnerabilities until a matrix like Table 1 is generated ($\tau_{r_i}(r_i)$ is set to be 1 here for convenience of the calculation).

3) In each row of Table 1, substitute $\tau_{r_j}(r_i)$ with $\tau(r_i/r_j)$, where $\tau(r_i/r_j) = \tau_{r_j}(r_i)/\max(\tau_{r_j}(r_i), \tau_{r_i}(r_j))$.

4) Finally, the vulnerable level of r_i is quantitatively characterized by $\sigma(r_i)$, $\sigma(r_i) = \min(\tau(r_i/r_1), \tau(r_i/r_2), \cdots, \tau(r_i/r_n))$.

DERFEM does not measure the vulnerable level of certain vulnerability directly, which could be difficult. It reveals the relatively vulnerable level of the vulnerability compared to the others.

2.2 Attack graph

In practice, a hacker may have to compromise a couple of interconnected hosts within a cyber system before he/she gains access to the control systems. For example, an outside intruder has to compromise an enterprise network, and then attacks its connected industrial control systems via the enterprise network. This procedure is modeled as an intrusion scenario in this research. An intrusion scenario is comprised of several intrusion actions, each action involves exploiting one security vulnerability.

An attack graph is employed to capture possible intrusion scenarios within a cyber system. The attack graph depicts ways in which a hacker compromises interconnected hosts sequentially by exploiting the corresponding vulnerabilities so as to achieve a specific goal. The benefits of the attack graph take into account the effects of interactions of local vulnerabilities and find global security holes introduced by the interconnections [9].

Basic concepts of the attack graph are defined as follows.

Definition 1: Subject (S^{T}). Subject is the initiator of actions. $S^{\mathrm{t}} \in S^{\mathrm{T}}$ can be an attacker or a compromised device.

Table 1 Comparison results of the vulnerabilities

Vulnerability	Scaled value				
	r_1	r_2	r_3	$\cdots$	r_l
r_1	1	$\tau_{r_2}(r_1)$	$\tau_{r_3}(r_1)$	$\cdots$	$\tau_{r_1}(r_1)$
r_2	$\tau_{r_1}(r_2)$	1	$\tau_{r_3}(r_2)$	$\cdots$	$\tau_{r_1}(r_2)$
r_3	$\tau_{r_1}(r_3)$	$\tau_{r_2}(r_3)$	1	$\cdots$	$\tau_{r_1}(r_3)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$
r_l	$\tau_{r_1}(r_l)$	$\tau_{r_2}(r_l)$	$\tau_{r_3}(r_l)$	$\cdots$	1

Definition 2: node (N^{D}). An electronic device in a cyber system is a node, using $n^{\mathrm{d}} = (i^{\mathrm{d}}), n^{\mathrm{d}} \in N^{\mathrm{D}}$ to denote. i^{d} is the identifier of the node, and it could be set as an equipment name. If a node is compromised by a subject, the node itself will become a subject.

Definition 3: privilege (P^{G}). It is used to describe the operating privilege of a subject in a node. When $s^{\mathrm{t}} \in S^{\mathrm{T}}$ and $n^{\mathrm{d}} \in N^{\mathrm{D}}$, the function $P^{\mathrm{G}}(S^{\mathrm{t}}, n^{\mathrm{d}}) \rightarrow \{0,1,2,3,4,5\}$ expresses the privilege level of s^{t} in n^{d}. $P^{\mathrm{G}}(s_i^t, n_j^{\mathrm{d}}) = 0$ implies that subject s_i^t has no access to node n_j^{d}; $P^{\mathrm{G}}(s_i^t, n_j^{\mathrm{d}}) = 1$ indicates that subject s_i^t is able to read the inbound and outbound messages of node n_j^{d}; $P^{\mathrm{G}}(s_i^t, n_j^{\mathrm{d}}) = 2$ means that subject s_i^t is able to block the inbound and outbound messages of node n_j^{d}; $P^{\mathrm{G}}(s_i^t, n_j^{\mathrm{d}}) = 3$ represents that subject s_i^t can read and block the inbound and outbound messages of node n_j^{d}; $P^{\mathrm{G}}(s_i^t, n_j^{\mathrm{d}}) = 4$ denotes that Subject s_i^t can send messages to node n_j^{d}; $P^{\mathrm{G}}(s_i^t, n_j^{\mathrm{d}}) = 5$ signifies that subject s_i^t has the full control access to node n_j^{d}.

Definition 4: state (Z). State is a triple $z = (s^t, n^{\mathrm{d}}, P^{\mathrm{G}}(s^t, n^{\mathrm{d}}))$. State is the prerequisite of the next attack action to be implemented.

Definition 5: interconnection (I^{C}). Interconnection refers to connections between nodes, using a quadruplet $i^{\mathrm{c}} = (n_i^{\mathrm{d}}, n_j^{\mathrm{d}}, C_{ij}, M_{ij})$, $i^{\mathrm{c}} \in I^{\mathrm{C}}$, $n_i^{\mathrm{d}}, n_j^{\mathrm{d}} \in N^{\mathrm{D}}$ to denote. C_{ij} represents the communication channel between n_i^{d} and n_j^{d}. C_{ij} could be copper wires, optical fibers, wireless, dial-up, virtual private network (VPN), or digital microwave. M_{ij} is the type of messages from n_i^{d} to n_j^{d}. M_{ij} could be measurements or control signals. M_{ij} does not necessarily equal to M_{ji}.

Definition 6: action (A). Action represents the set of possible actions of the subjects in a cyber system. Action is a quadruplet $a = (n_{\mathrm{name}}, z_{\mathrm{s}}, z_{\mathrm{d}}, \gamma)$, $a \in A$, $z_{\mathrm{s}}, z_{\mathrm{d}} \in Z$. n_{name} is the name of an attack action such as the denial-of-service (DOS) attack or the man-in-the-middle attack; z_{s} and z_{d} represent the initial and final states of the action; γ is the vulnerability exploited in the action. γ is used to denote the difficult level of action a.

The algorithm to construct an attack graph proceeds as follows.

1) Identify N^{D} and I^{C}. Develop a directed graph (N^{D}, I^{C}). The vertex is $n^{\mathrm{d}} \in N^{\mathrm{D}}$, and the edge is $i^{\mathrm{c}} \in I^{\mathrm{C}}$.

2) Identify the node n_k^{d} which will be the target of attacks. n_k^{d} could be a SCADA server or a programmable logic controller (PLC).

3) Determine the goals of attacks—the state of n_k^{d} after being attacked, formulated as follows: $z_{\mathrm{d}} = (s_i^{\mathrm{t}}, n_k^{\mathrm{d}}, P^{\mathrm{G}}(s_i^{\mathrm{t}}, n_k^{\mathrm{d}}) > 0)$, in which s_i^{t} represents the initial intruding subject (hackers).

4) Traverse the directed graph (N^{D}, I^{C}). Identify the node $n_{k'}^{\mathrm{d}}$ that is connected to n_k^{d} directly. Assume that node $n_{k'}^{\mathrm{d}}$ has been compromised by s_i^{t}, and it becomes an intruding subject, say $s_{i'}^{\mathrm{t}}$.

5) Extract an attack action aimed at n_k^{d} from $s_{i'}^{\mathrm{t}}$, such that $a = (n_{\mathrm{name}}, z_{\mathrm{s}}, z_{\mathrm{d}}, \gamma_{\mathrm{a}})$, $z_{\mathrm{d}} = (s_{i'}^{\mathrm{t}}, n_k^{\mathrm{d}}, P^{\mathrm{G}}(s_{i'}^{\mathrm{t}}, n_k^{\mathrm{d}}) = P^{\mathrm{G}}(s_i^{\mathrm{t}}, n_k^{\mathrm{d}}))$. γ_{a} is the vulnerability of node n_k^{d} exploited in action a.

6) Establish the prerequisite of action a: z_{s}, formulated as follows: $z_{\mathrm{s}} = (s_i^{\mathrm{t}}, n_{k'}^{\mathrm{d}}, P^{\mathrm{G}}(s_i^{\mathrm{t}}, n_{k'}^{\mathrm{d}}) > 0)$.

7) Set $n_{k'}^{\mathrm{d}}$ as a new target node, and z_{s} becomes another z_{d}. Repeat step 4, 5 and 6, until $s_{i'}^{\mathrm{t}} = s_i^{\mathrm{t}}$.

After the attack graph is built, it gives a bird's-eye view of possible intrusion scenarios. For each scenario, the probability of occurrence P^{b} is calculated as follows.

a) If the intrusion scenario is comprised of two serial intrusion actions a_i and a_j, then

$$P^{\mathrm{b}} = \sigma(\gamma_{a_i})\sigma(\gamma_{a_j}) \tag{1}$$

where γ_{a_i} and γ_{a_j} are the local vulnerabilities exploited in the attack actions a_i and a_j. Note that P^{b} is relative as $\sigma(\gamma_{a_i})$ and $\sigma(\gamma_{a_j})$ are relative. P^{b} tells how possible an intrusion scenario is compared to the others.

b) If the intrusion scenario consists of two parallel intrusion actions a_i and a_j, then

$$P^{\mathrm{b}} = \sigma(\gamma_{a_i}) + \sigma\left(\gamma_{a_j}\right) - \sigma(\gamma_{a_i})\sigma(\gamma_{a_j}) \tag{2}$$

c) If the intrusion scenario is more complicated, the calculation of its P^{b} will be the synthesis of (1) and (2).

2.3 Intrusion response system

The concept of IRS is illustrated in Fig. 2. It is intended to be an application in the control center of a power system. The proposed algorithm, which will be discussed in detail in Section 3, obtains updated power network configurations from the state estimator (SE), say, every 5 minutes. If an intrusion scenario is executed successfully, and it results in disruptions in power system operations such as breaker opening or loss of generation, such sudden changes of the power network configurations will be reported to the proposed algorithm through SCADA systems in real time. The post-attack dynamical model of the power system is then built. After that, the algorithm extracts synchronized phasor measurements from the PMU data concentrator, which obtains real time PMU data from substations equipped with PMUs. A number of the state variables of the dynamical model are observed from PMU data. Based on the dynamical model and PMU measurements, CLEs are calculated to monitor the impact of the intrusion on power system dynamics.

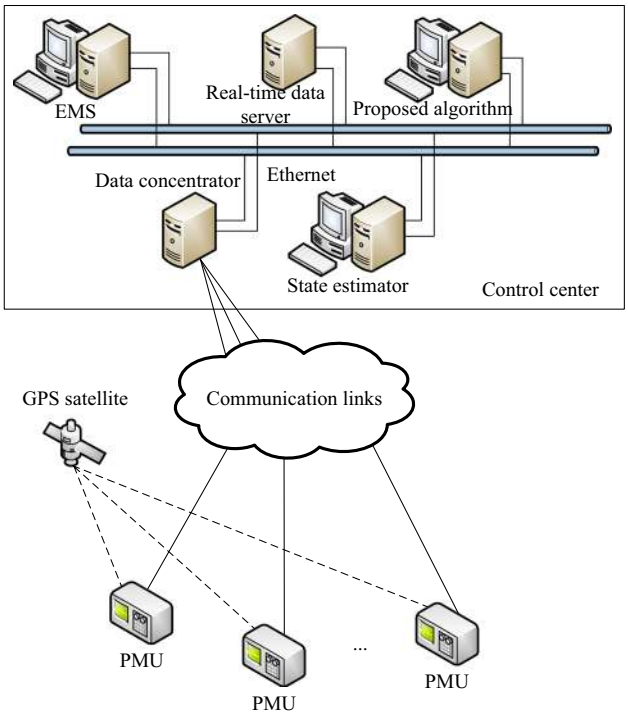

Fig. 2 Concept of IRS

If CLEs have only low values, the prediction is that voltage instability will not happen; otherwise, voltage instability is likely to occur, and the proposed algorithm will send proper control signals to the energy management system (EMS) to prevent voltage instability.

3 Proposed algorithm

3.1 Dynamical model

In this algorithm, generators are represented by classical models, and loads are represented by ZIP models. After a cyber intrusion, the dynamical model of a power system is established as shown below:

$$\begin{cases} \boldsymbol{Y}_{\mathrm{bus}}\dot{\boldsymbol{V}} = \dot{\boldsymbol{I}} \\ -\dot{V}_i\dot{I}_i^* = P_{\mathrm{D},i} + \mathrm{j}Q_{\mathrm{D},i} \\ \dot{V}_j\dot{I}_j^* = \dot{V}_j\left(\frac{\Omega_j\angle\delta_j - \dot{V}_j}{Z_j}\right)^* \end{cases} \tag{3}$$

$$\begin{cases} \frac{\mathrm{d}\delta_j}{\mathrm{d}t} = \omega_j \\ \frac{2H_j}{\omega_{\mathrm{Re}}}\frac{\mathrm{d}\omega_j}{\mathrm{d}t} + \frac{O_j}{\omega_{\mathrm{Re}}}\omega_j = P_{\mathrm{m},j} - \mathrm{Re}((\Omega_j\angle\delta_j)\dot{I}_j^*) \end{cases} \tag{4}$$

where $i = 1, 2, \cdots, n-m$; $j = n-m+1, n-m+2, \cdots, n$; n is the total number of buses; m is the total number of generators; $P_{\mathrm{D},i} + \mathrm{j}Q_{\mathrm{D},i}$ is the power consumption at

load bus i; $P_{\mathrm{D},i} = P_{0,i}\left[A_i + B_i\left(\frac{|V_i|}{|V_{0,i}|}\right) + C_i\left(\frac{|V_i|}{|V_{0,i}|}\right)^2\right]$ $\left(1 + L_{P,i}\Delta f\right)$; $Q_{\mathrm{D},i} = Q_{0,i}\left[D_i + E_i\left(\frac{|V_i|}{|V_{0,i}|}\right) + F_i\left(\frac{|V_i|}{|V_{0,i}|}\right)^2\right]$ $\left(1 + L_{Q,i}\Delta f\right)$; A_i, B_i, C_i, D_i, E_i, F_i, $L_{P,i}$, and $L_{Q,i}$ are load parameters; $P_{0,i} + \mathrm{j}Q_{0,i}$ is the steady-state power consumption; $V_{0,i}$ is the steady-state voltage; Δf is the frequency deviation in p.u.; H_j and O_j are generator inertias; δ_j is the rotor angle of generator j; ω_j is the angular speed of generator j; ω_{Re} is the reference speed; Ω_j is the internal voltage magnitude at generator j; Z_j is the impedance between generator j and its generator bus; $P_{\mathrm{m},j}$ is the mechanical power input to generator j.

Excitation systems of the generators are assumed to function in some way to keep internal voltage magnitudes at reference values during the transient period. The time constant of modern excitation systems is less than 0.5 s. If a new reference value is issued to an excitation system, the corresponding voltage magnitude will change rapidly due to the fast response of the excitation system. CLEs will be computed based on an updated dynamical model to reassess system stability.

Let $\boldsymbol{x}$ denote $[|V_1|, \angle V_1, |V_2|, \angle V_2, \cdots, |V_n|, \angle V_n]^{\mathrm{T}}$, and $\boldsymbol{y}$ denote $[\delta_1, \omega_1, \cdots, \delta_m, \omega_m]^{\mathrm{T}}$. Equations (3) and (4) are represented by:

$$\boldsymbol{G}(\boldsymbol{x}, \boldsymbol{y}) = 0 \tag{5}$$

$$\frac{\mathrm{d}\boldsymbol{y}}{\mathrm{d}t} = \boldsymbol{F}(\boldsymbol{x}, \boldsymbol{y}) \tag{6}$$

Since

$$\frac{\mathrm{d}\boldsymbol{G}(\boldsymbol{x}, \boldsymbol{y})}{\mathrm{d}t} = 0 = \boldsymbol{G}_{\boldsymbol{x}}\frac{\mathrm{d}\boldsymbol{x}}{\mathrm{d}t} + \boldsymbol{G}_{\boldsymbol{y}}\frac{\mathrm{d}\boldsymbol{y}}{\mathrm{d}t} \tag{7}$$

It is obtained that:

$$\frac{\mathrm{d}\boldsymbol{x}}{\mathrm{d}t} = -(\boldsymbol{G}_{\boldsymbol{x}})^{-1}\boldsymbol{G}_{\boldsymbol{y}}\frac{\mathrm{d}\boldsymbol{y}}{\mathrm{d}t} = -(\boldsymbol{G}_{\boldsymbol{x}})^{-1}\boldsymbol{G}_{\boldsymbol{y}}\boldsymbol{F}(\boldsymbol{x}, \boldsymbol{y}) \tag{8}$$

where $\boldsymbol{G}_{\boldsymbol{x}}$ and $\boldsymbol{G}_{\boldsymbol{y}}$ are the Jacobian matrixs of $\boldsymbol{G}$ with respect to $\boldsymbol{x}$ and $\boldsymbol{y}$.

When $\det(\boldsymbol{G}_{\boldsymbol{x}}) = 0$ and $\boldsymbol{G}_{\boldsymbol{y}}\frac{\mathrm{d}\boldsymbol{y}}{\mathrm{d}t} \neq 0$, $\frac{\mathrm{d}\boldsymbol{x}}{\mathrm{d}t}$ has very large values. Correspondingly, $\boldsymbol{x}$ will change dramatically, and voltage instability is likely to happen.

3.2 Methodology: CLEs

The notion of CLEs (originally called sub-Lyapunov exponents) is introduced by Pecora and Carroll in their study of synchronization of chaotic systems [10] and [11]. Similar to the full Lyapunov exponents, CLEs are well defined ergodic invariants.

Consider a N-dimensional continuous-time dynamical system $\frac{\mathrm{d}\boldsymbol{z}}{\mathrm{d}t} = \boldsymbol{H}(z)$. Split the state vector $\boldsymbol{z}$ into two vectors: $\boldsymbol{z}_1 \in \mathbf{R}^K$, and $\boldsymbol{z}_2 \in \mathbf{R}^{N-K}$ $(0 < K < N)$, one will obtain two sub systems: $\frac{\mathrm{d}\boldsymbol{z}_1}{\mathrm{d}t} = \boldsymbol{H}_1(\boldsymbol{z}_1, \boldsymbol{z}_2)$ and $\frac{\mathrm{d}\boldsymbol{z}_2}{\mathrm{d}t} = \boldsymbol{H}_2(\boldsymbol{z}_1, \boldsymbol{z}_2)$. Let $\boldsymbol{z}_1(t) = \boldsymbol{\varphi}(t, \boldsymbol{v}_1, \boldsymbol{v}_2)$ be the solution of the first sub system at time t starting from the initial conditions $\boldsymbol{z}_1^0 = \boldsymbol{v}_1$, $\boldsymbol{z}_2^0 = \boldsymbol{v}_2$. The CLEs C_i for the sub system $\frac{\mathrm{d}\boldsymbol{z}_1}{\mathrm{d}t} = \boldsymbol{H}_1(\boldsymbol{z}_1, \boldsymbol{z}_2)$ are defined as eigenvalues of the following limiting.

$$\boldsymbol{\Lambda}(\boldsymbol{v}_1) = \lim_{t\to\infty}[\boldsymbol{K}^{\mathrm{T}}(t, \boldsymbol{v}_1, \boldsymbol{v}_2)\boldsymbol{K}(t, \boldsymbol{v}_1, \boldsymbol{v}_2)]^{\frac{1}{2t}} \tag{9}$$

$$C_i(\boldsymbol{v}_1) = \ln(\bar{\lambda}_i(\boldsymbol{v}_1)) \tag{10}$$

where $i = 1, 2, \cdots, K$; $\boldsymbol{K}(t, \boldsymbol{v}_1, \boldsymbol{v}_2)$ is the Jacobian matrix of $\boldsymbol{\varphi}(t, \boldsymbol{v}_1, \boldsymbol{v}_2)$ with respect to $\boldsymbol{v}_1$; $\bar{\lambda}_i(\boldsymbol{v}_1)$ is the ith eigenvalue of $\boldsymbol{\Lambda}(\boldsymbol{v}_1)$. The existence of CLEs is guaranteed under the same conditions that establish the existence of the Lyapunov exponents [12].

The relationship between CLEs and system stability is discussed in the following. In ergodic theory of dynamical systems, the Lyapunov exponents are used to characterize the exponential divergence or convergence of nearby trajectories, as shown in Fig. 3. For the sub system $\frac{\mathrm{d}\boldsymbol{z}_1}{\mathrm{d}t} = \boldsymbol{H}_1(\boldsymbol{z}_1, \boldsymbol{z}_2)$, its maximal conditional Lyapunov exponent (MCLE) M_{MCLE} determines the exponential convergence of nearby system trajectories. This is true due to the approximation of

$$\|\Delta\boldsymbol{z}_1(t)\| \approx e^{M_{\mathrm{MCLE}}t}\left\|\Delta\boldsymbol{z}_1^0\right\| \tag{11}$$

If $\frac{\mathrm{d}\boldsymbol{z}_1}{\mathrm{d}t}$ has very large values, the nearby system trajectories will diverge. Correspondingly, $M_{\mathrm{MCLE}} \gg 0$. Otherwise, the nearby trajectories will converge, and MCLE has a low or even negative value. Therefore, the value of MCLE reveals the magnitude of time derivatives of related state variables. When the state variables are

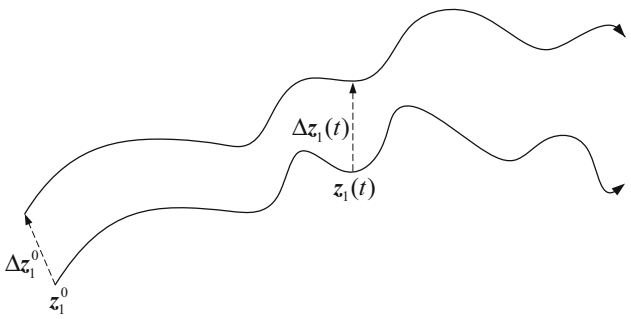

Fig. 3 Nearby trajectories in the state space

voltages of a power system, MCLE can be used to monitor the magnitude of time derivatives of the voltages, and hence voltage stability.

In this work, the dynamical system in (8) is split into n sub systems. The ith sub system has the state variables $[|V_i|, \angle V_i]^{\mathrm{T}}$, where $i = 1, 2, \cdots, n$. MCLE is computed for each sub system to monitor voltage stability within it.

Let $\boldsymbol{G}_{\boldsymbol{y}} \frac{\mathrm{d}\boldsymbol{y}}{\mathrm{d}t} = \boldsymbol{\Phi} \in \mathbf{R}^{2n}$, one may obtain

$$\begin{cases} \boldsymbol{\Phi}_{2i-1} = \frac{|V_i|\Omega_i \cos(\angle(V_i + Z_i - \delta_i))}{|Z_i|} \frac{\mathrm{d}\delta_i}{\mathrm{d}t} \\ \quad + Q_{0,i}\left[D_i + E_i\left(\frac{|V_i|}{|V_{0,i}|}\right) + F_i\left(\frac{|V_i|}{|V_{0,i}|}\right)^2\right] L_{Q,i} \frac{\mathrm{d}\Delta f}{\mathrm{d}t} \\ \boldsymbol{\Phi}_{2i} = -\frac{|V_i|\Omega_i \sin(\angle(V_i + Z_i - \delta_i))}{|Z_i|} \frac{\mathrm{d}\delta_i}{\mathrm{d}t} \\ \quad + P_{0,i}\left[A_i + B_i\left(\frac{|V_i|}{|V_{0,i}|}\right) + C_i\left(\frac{|V_i|}{|V_{0,i}|}\right)^2\right] L_{P,i} \frac{\mathrm{d}\Delta f}{\mathrm{d}t} \end{cases} \tag{12}$$

where $i = 1,2,\ldots,n$. $\Omega_{\mathrm{i}} = 0$, $|Z_i| = \infty$, and $\delta_i = 0$ if there is no generator at bus i.

As $\frac{\mathrm{d}\Delta f}{\mathrm{d}t}$ is small,

$$\begin{cases} \boldsymbol{\Phi}_{2i-1} \approx \frac{|V_i|\Omega_i \cos(\angle(V_i + Z_i - \delta_i))}{|Z_i|} \omega_i \\ \boldsymbol{\Phi}_{2i} \approx -\frac{|V_i|\Omega_i \sin(\angle(V_i + Z_i - \delta_i))}{|Z_i|} \omega_i \end{cases} \tag{13}$$

One can assume that $\boldsymbol{G}_{\boldsymbol{x}}$ is diagonal in computation without compromising the accuracy, and then the ith sub system of (8) is represented by:

$$\begin{aligned} \frac{\mathrm{d}|V_i|}{\mathrm{d}t} &= -\frac{\boldsymbol{\Phi}_{2i-1}}{\boldsymbol{G}_{\boldsymbol{x}}(2i-1, 2i-1)} \\ \frac{\mathrm{d}\angle V_i}{\mathrm{d}t} &= -\frac{\boldsymbol{\Phi}_{2i}}{\boldsymbol{G}_{\boldsymbol{x}}(2i, 2i)} \end{aligned} \tag{14}$$

where $i = 1, 2,\ldots,n$; $\boldsymbol{G}_{\boldsymbol{x}}(2i - 1, 2i - 1)$ is the element at row $2i - 1$ and column $2i - 1$ of $\boldsymbol{G}_{\boldsymbol{x}}$. It is noted that $\frac{\mathrm{d}|V_i|}{\mathrm{d}t} = \frac{\mathrm{d}\angle V_i}{\mathrm{d}t} = 0$ if there is no generator at bus i, which is reasonable since the change of the voltages at load buses is driven by the voltages at generator buses. Consequently, $\frac{\mathrm{d}|V_i|}{\mathrm{d}t}$ and $\frac{\mathrm{d}\angle V_i}{\mathrm{d}t}$ do not depend on $|V_i|$ and $\angle V_i$.

The proposed algorithm calculates MCLEs of the sub systems that have generators at the corresponding buses. The computation method is introduced in the following.

3.3 Computation method

MCLEs are calculated over a limited time window. PMU measurements are extracted to observe time-varying values of the state variables of the sub systems. The unobservable part of the state variables is approximated through the implicit integration method with trapezoidal rule [13]. At the same time, the observable part is estimated by the same method as a backup of PMU data. If a PMU is compromised, it will be detected by comparing the PMU data and the corresponding estimation results. The estimation results will be used in the MCLE calculation. The algorithm in [13], the standard method with Gram-Schmidt reorthonormalization (GSR), is then used to compute MCLEs. If the values of MCLEs are over a predefined limit, it is predicted that voltage instability will happen. Control signals will be sent to EMS to prevent the voltage instability.

Selection of the length of the time interval could be arbitrary. Study shows that MCLEs exhibit robustness to the length of the time interval: MCLEs computed over different length time intervals all have very high values if voltage instability is going to happen. In this research, the time interval length is set to be 0.2 s, so that it is short while it has enough PMU measurements.

3.4 Control actions

When the value of MCLE of a sub system is over a predefined limit, the proposed algorithm will send a control signal to the excitation system of the generator related to the sub system through EMS. The reference value of the generator internal voltage magnitude is modified as follows:

$$\boldsymbol{\Omega}_{\mathrm{Gen}}^{\mathrm{ref,new}} = \left(1 + \frac{M_{\mathrm{MCLE}}}{C_{\mathrm{const}}}\right) \boldsymbol{\Omega}_{\mathrm{Gen}}^{\mathrm{ref,old}} \tag{15}$$

where C_{const} is a predefined constant value. Voltage instability can be prevented with the fast response of the exciting system.

4 Case study

Wind farm SCADA systems are selected for case study due to the fact that wind power is a fast-emerging renewable resource on power grids, and it has the potential to affect the dynamical performance of power systems.

4.1 Wind farm SCADA systems

The generic network configuration of wind farm SCADA systems is identified and shown in Fig. 4. Every wind turbine is equipped with a wind turbine control panel (WTCP), which monitors and controls the wind turbine. WTCP is normally mounted in the tower base and is easily accessible. Through WTCPs, servers in a control room support monitoring and control of the wind turbines within a wind farm. However the control room is normally not

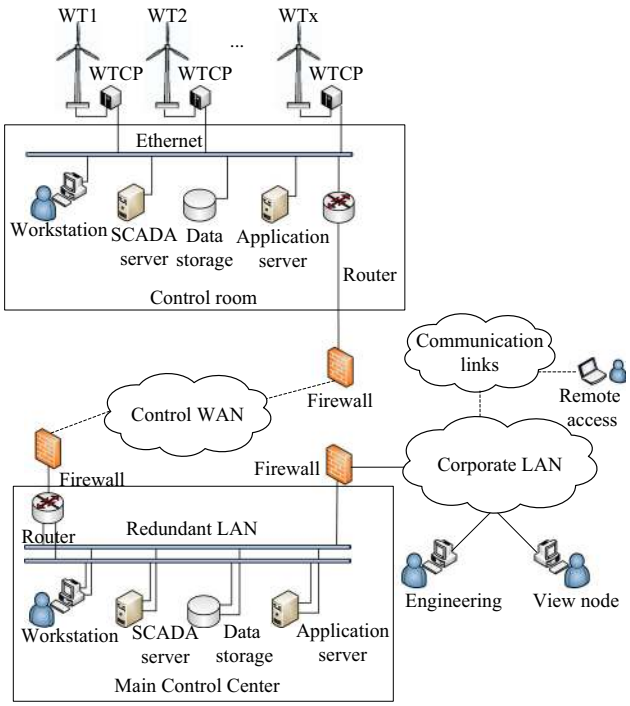

Fig. 4 Generic network configuration of wind farm SCADA systems

staffed and it is only for maintenance occasions. Wind farms in separate locations are integrated into a single EMS in a main control center through a control wide area network (WAN). In the control center, system analysts oversee every turbine at the wind farms. The control center interfaces restrictively with corporate networks for business and operational reasons.

Vulnerabilities are identified in [14], including configuration management of WTCPs (r_1), implicit trust between WTCPs and a control room (r_2), implicit trust between control rooms and a control center (r_3), wireless network (r_4), optical fibers (r_5), virtual private network (r_6), digital microwave (r_7), poor access control within a control room (r_8), poor access control within a control center (r_9), bad configuration of remote access (r_{10}), weak firewall policy (r_{11}), and human errors (r_{12}).

The vulnerabilities are evaluated through DERFEM. The results are shown in Table 2. An attack graph is built as shown in Fig. 5. Nine possible intrusion scenarios are identified, and the probability of occurrence of every scenario is calculated, as shown in Table 3.

The intrusion scenarios show that, if successfully executed, a hacker will gain some levels of control access to several or even hundreds of WTCPs. The output of compromised wind farms will be maliciously manipulated. The impact on power system dynamics is studied next.

In Fig. 5, z_1 = (hacker, WTCP, 5); z_2 = (hacker, WTCP, 0); z_3 = (hacker, WTCPs in a wind farm, 2); z_4 = (hacker, WTCPs in a wind farm, 0); z_5 = (hacker, WTCPs in a wind farm, 1); z_6 = (hacker, WTCPs in a wind farm, 4); z_7 = (hacker, SCADA server in the control room, 3); z_8 = (hacker, SCADA server in the control room, 0); z_9 = (hacker, SCADA server in the control room, 4); z_{10} = (hacker, SCADA server in the control center, 2); z_{11} = (hacker, SCADA server in the control center, 0); z_{12} = (hacker, SCADA server in the control room, 5); z_{13} = (hacker, workstation in the control room, 5); z_{14} = (hacker, workstation in the control room, 0); z_{15} = (hacker, SCADA server in the control center, 5); z_{16} = (hacker, workstation in the control center, 5); z_{17} = (hacker, workstation in the control center, 0); z_{18} = (hacker, workstation in the corporate LAN, 5); z_{19} = (hacker, workstation in the corporate LAN, 0); z_{20} = (hacker, remote access point, 5); z_{21} = (hacker, remote access point, 0); a_1 = (password cracking, z_2, z_1, r_1); a_2 = (jamming, z_4, z_3, r_4); a_3 = (passive tapping, z_4, z_5, r_5); a_4 = (man-in-the-middle attack, z_7, z_6, r_2); a_5 = (active tapping, z_8, z_7, r_5); a_6 = (spoof, z_9, z_6, r_2); a_7 = (spoof, z_{10}, z_9, r_3); a_8 = (DOS attack, z_{11}, z_{10}, r_6); a_9 = (jamming, z_{11}, z_{10}, r_7); a_{10} = (spoof, z_{12}, z_6, r_2); a_{11} = (internal attack, z_8, z_{12}, r_{12}); a_{12} = (malware infection, z_{13}, z_{12}, r_8); a_{13} = (infected portable storage device attack, z_{14}, z_{13}, r_{12}); a_{14} = (malware infection, z_{15}, z_{12}, r_3); a_{15} = (malware infection, z_{16}, z_{15}, r_9); a_{16} = (infected portable storage device attack, z_{17}, z_{16}, r_{12}); a_{17} = (malware infection, z_{18}, z_{16}, r_{11}); a_{18} = (infected portable storage device attack, z_{19}, z_{18}, r_{12}); a_{19} = (phishing, z_{19}, z_{18}, r_{12}); a_{20} = (malware infection, z_{20}, z_{18}, r_{10}); a_{21} = (infected portable storage device attack, z_{21}, z_{20}, r_{12}); a_{22} = (phishing, z_{21}, z_{20}, r_{12}).

4.2 Simulation results

The IEEE 39 bus system [15] shown in Fig. 6 is used for simulations. Generator G5 and G9 (marked with two rectangles) are replaced by two wind farms comprised of hundreds of variable speed wind turbines utilizing the doubly-fed induction generators (DFIGs). The rating of each wind turbine is 2.0 MW. From the system point of view, the wind farms are considered as constant negative loads during the transient period, due to the fast control capacity of the power electronic technology within wind turbines. The other generators are classically modeled and the loads are represented by ZIP models.

MCLEs are calculated for the generator buses (except G5 and G9) by the proposed algorithm every 0.2 s to monitor power system stability. Assume that at $t = 0.4$ s, a hacker maliciously manipulates the power output of G5 (or G9) to some extent. Part of the simulation results is shown in Table 4.

The explains of Table 4 are as following.

Table 2 Results of DERFEM

Vulnerability	r_1	r_2	r_3	r_4	r_5	r_6	r_7	r_8	r_9	r_{10}	r_{11}	r_{12}	$\sigma(r_2)$
r_1	1	0.8	0.8	0.8	0.8	0.8	0.8	0.8	0.8	0.8	0.8	0.8	1.0
r_2	0.6	1	0.9	0.7	0.5	0.8	0.8	0.6	0.6	0.5	0.6	0.4	0.75
r_3	0.4	0.6	1	0.5	0.4	0.7	0.8	0.3	0.2	0.3	0.2	0.5	0.50
r_4	0.5	0.4	0.6	1	0.7	0.7	0.7	0.6	0.5	0.4	0.6	0.5	0.5714
r_5	0.4	0.3	0.3	0.4	1.0	0.3	0.3	0.5	0.5	0.6	0.5	0.6	0.50
r_6	0.2	0.2	0.3	0.2	0.2	1.0	0.3	0.2	0.2	0.3	0.2	0.2	0.25
r_7	0.1	0.1	0.2	0.1	0.1	0.1	1.0	0.1	0.1	0.2	0.1	0.1	0.125
r_8	0.5	0.5	0.5	0.5	0.4	0.6	0.3	1.0	0.4	0.5	0.4	0.4	0.625
r_9	0.2	0.3	0.1	0.3	0.2	0.2	0.2	0.2	1.0	0.2	0.2	0.1	0.25
r_{10}	0.7	0.4	0.6	0.5	0.4	0.6	0.5	0.6	0.6	1.0	0.6	0.4	0.6667
r_{11}	0.4	0.5	0.4	0.5	0.4	0.5	0.3	0.5	0.5	0.5	1.0	0.5	0.5
r_{12}	0.3	0.3	0.4	0.3	0.3	0.2	0.2	0.3	0.3	0.3	0.2	1.0	0.375

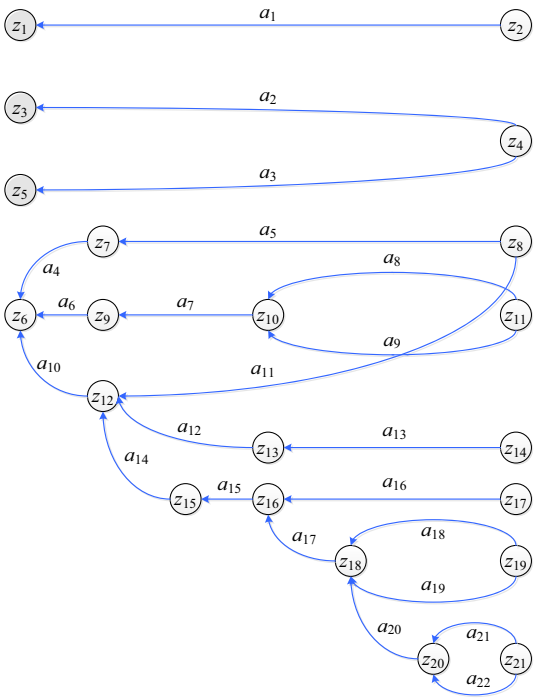

Fig. 5 Constructed attack graph

Attack 1: P_{Gen} of G5 is reduced by 10 MW. Attack 2: Q_{Gen} of G5 is reduced by 10 Mvar. Attack 3: P_{Gen} of G5 is reduced by 100 MW. Attack 4: Q_{Gen} of G5 is reduced by 100 Mvar. Attack 5: P_{Gen} of G9 is reduced by 10 MW. Attack 6: Q_{Gen} of G9 is reduced by 7.5 Mvar. Attack 7: P_{Gen} of G9 is reduced by 100 MW. Attack 8: Q_{Gen} of G9 is reduced by 75 Mvar. Attack 9: P_{Gen} of G5 is reduced by half. Attack 10: Q_{Gen} of G5 is reduced by half. Attack 11: Q_{Gen} of G5 is reduced to -Q_{Gen}. Attack 12: P_{Gen} of G9 is reduced by half. Attack 13: P_{Gen} of G5 is reduced by half.

Table 3 Intrusion scenarios and probabilities

Intrusion scenario	P^{b}
a_1	1
a_2	0.5714
a_3	0.5
$a_5 \rightarrow a_4$ or $a_{11} \rightarrow a_{10}$	0.5508
a_8 (or a_9) $\rightarrow a_7 \rightarrow a_6$	0.1289
$a_{13} \rightarrow a_{12} \rightarrow a_{10}$	0.1758
$a_{16} \rightarrow a_{15} \rightarrow a_{14} \rightarrow a_{10}$	0.0352
a_{18} (or a_{19}) $\rightarrow a_{17} \rightarrow a_{15} \rightarrow a_{14} \rightarrow a_{10}$	0.0176
a_{21} (or a_{22}) $\rightarrow a_{20} \rightarrow a_{17} \rightarrow a_{15} \rightarrow a_{14} \rightarrow a_{10}$	0.0117

Q_{Gen} of G5 is reduced by half. P_{Gen} of G9 is reduced by half. Attack 14: P_{Gen} of G5 is reduced by 30 MW. Q_{Gen} of G5 is reduced by15 Mvar. P_{Gen} of G9 is reduced by 50 MW. Q_{Gen} of G9 is reduced by 10 Mvar.

The simulation results come to the following conclusions.

1) The values of MCLEs are close to 0, when the power system is in the steady state.

2) Upon an attack, the values of MCLEs oscillate as time evolves, but have limited values if voltage instability is not likely to happen. During Attack 2, the reactive power output of G5 is reduced by 10 Mvar at $t = 0.4$ s. MCLEs increase for a while, and then decrease, as shown in Fig. 7a. The values are below 200.

3) The values of MCLEs constantly increase as time evolves, if voltage instability is likely to happen within the power system. During Attack 10, the reactive power output of G5 is reduced by half at $t = 0.4$ s. Voltage instability happens at $t = 1.42$ s, as shown in Fig. 7b. The values of MCLEs keep increasing after the attack, as shown in Fig. 7c.

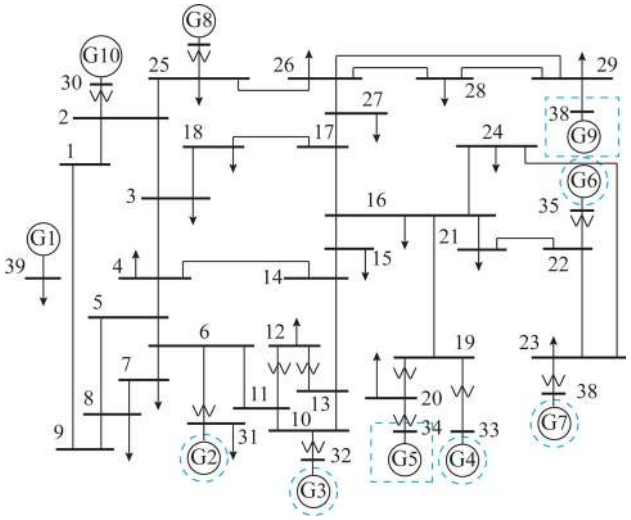

Fig. 6 IEEE 10 generator 39 bus system

4) Voltage instability is likely to occur around the generator buses where MCLEs have high values. Take Attack 10 as an example, MCLEs of G2, G3, G4, G6 and G7 (circled in Fig. 6) are over 1000 at $t = 1.4$ s. Time-domain simulation results show that voltage instability happens around those generator buses. It is reasonable as G2, G3, G4, G6 and G7 are close to G5.

Based on the simulation results, a predefined limit for the values of MCLEs is set to be 800. If the value of MCLE of a generator bus exceeds the limit, it is predicted that voltage instability will happen around the generator bus. Control signal

$$\boldsymbol{\Omega}_{\text{Gen}}^{\text{ref,new}} = \left(1 + \frac{M_{\text{MCLE}}}{10000}\right)\boldsymbol{\Omega}_{\text{Gen}}^{\text{ref,old}} \tag{15}$$

will be sent to the excitation system of the related generator. Simulation results show that voltage instability can be avoided. For example, during Attack 10, MCLEs of G3, G4, G6 and G7 are over 800 at $t = 1.2$ s. The corresponding control signals are then sent to G3, G4, G6 and G7. Voltage instability is prevented, as shown in Fig. 7d.

5 Conclusion

A risk assessment framework with a PMU-based IRS is proposed for power control systems. The main idea of IRS is to calculate MCLEs for generator buses in order to monitor voltage stability. The higher values MCLEs have, the more likely voltage instability occur around the corresponding generator buses. MCLE method is based on a solid analytical foundation and it is validated by simulation results.

This research leads to significant contributions to the development of a more reliable and secure power grid. Future research includes the following aspects.

1) For a large cyber system with numerous security vulnerabilities, DERFEM may not be sufficient. Some statistical analysis techniques may be coupled with DERFEM to improve evaluation results.

2) A dedicated control strategy will be developed in IRS for control actions to prevent voltage instability. The voltages are over 1.2 after 1.8 s in Fig. 7d. It is because IRS employs a control action on a simplified excitation system. The dedicated control strategy will be studied with full-scale excitation systems.

Table 4 MCLE of bus G3

Attack	MCLE									Voltage instability
	0 ~ 0.2 s	0.2 ~ 0.4 s	0.4 ~ 0.6 s	0.6 ~ 0.8 s	0.8 ~ 1 s	1 ~ 1.2 s	1.2 ~ 1.4 s	1.4 ~ 1.6s	1.6 ~ 1.8 s	
1	-2.77×10^{-3}	-2.62×10^{-2}	9.88×10^{-1}	2.77	3.84	3.69	2.96	3.55	7.29	N/A
2	-2.77×10^{-3}	-2.62×10^{-2}	7.25	2.81×10	6.23×10	1.14×10^{2}	1.90×10^{2}	1.83×10^{2}	6.98×10	N/A
3	-2.77×10^{-3}	-2.62×10^{-2}	6.90×10	2.11×10^{2}	3.94×10^{2}	6.83×10^{2}	1.22×10^{3}			$t = 1.57$ s
4	-2.77×10^{-3}	-2.62×10^{-2}	1.17×10^{2}	4.08×10^{2}	9.12×10^{2}	1.98×10^{3}				$t = 1.20$ s
5	-2.77×10^{-3}	-2.62×10^{-2}	-1.01	-2.27	-3.16	-4.08	-4.58	-4.23	-2.78	N/A
6	-2.77×10^{-3}	-2.62×10^{-2}	6.04	2.21×10	4.65×10	8.18×10	1.32×10^{2}	1.09×10^{2}	4.81	N/A
7	-2.77×10^{-3}	-2.62×10^{-2}	3.45×10	1.05×10^{2}	2.00×10^{2}	3.51×10^{2}	6.12×10^{2}	1.10×10^{3}	2.17×10^{3}	$t = 1.86$ s
8	-2.77×10^{-3}	-2.62×10^{-2}	1.05×10^{2}	3.48×10^{2}	7.27×10^{2}	1.43×10^{3}				$t = 1.24$ s
9	-2.77×10^{-3}	-2.62×10^{-2}	2.31×10^{2}	7.65×10^{2}	1.72×10^{3}					$t = 1.03$ s
10	-2.77×10^{-3}	-2.62×10^{-2}	7.12×10	2.45×10^{2}	5.27×10^{2}	1.03×10^{3}	2.05×10^{3}			$t = 1.42$ s
11	-2.77×10^{-3}	-2.62×10^{-2}	3.55×10^{2}	1.37×10^{3}						$t = 0.8$ s
12	-2.77×10^{-3}	-2.62×10^{-2}	2.91×10^{2}	1.03×10^{3}	2.72×10^{3}					$t = 1.06$ s
13	-2.77×10^{-3}	-2.62×10^{-2}	8.33×10^{2}							$t = 0.76$ s
14	-2.77×10^{-3}	-2.62×10^{-2}	6.43×10	2.07×10^{2}	4.10×10^{2}	7.47×10^{2}	1.38×10^{3}			$t = 1.56$ s

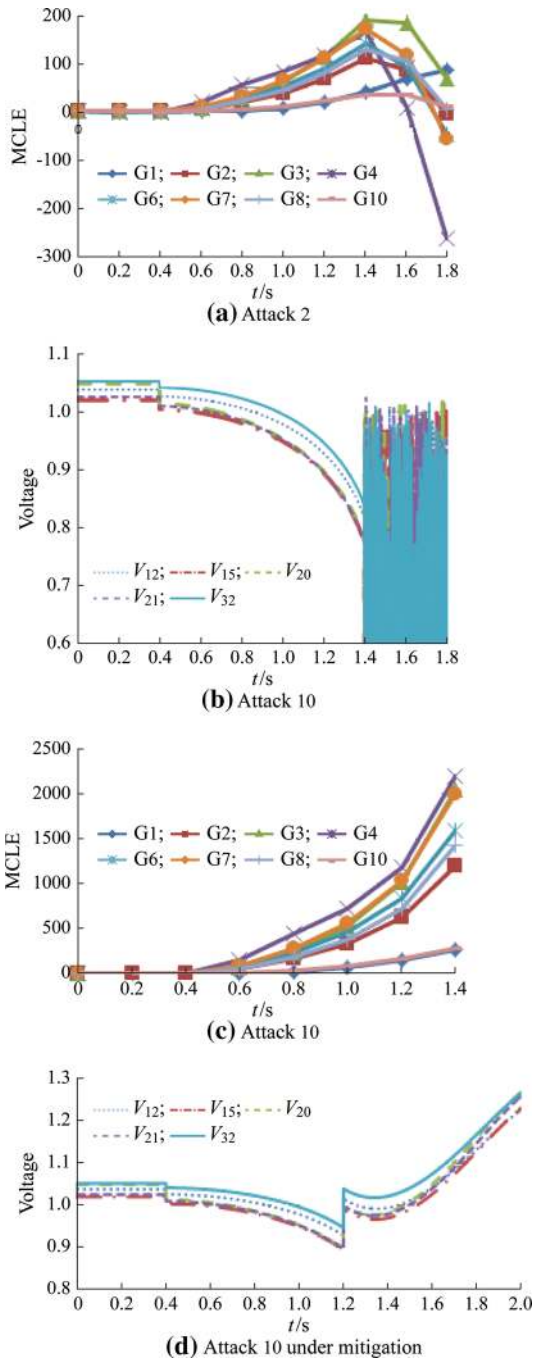

Fig. 7 Simulation results

3) IRS is not only able to monitor voltage stability under cyber intrusions, but also can be used to monitor voltage stability after disturbances. It is promising to integrate IRS and the on-line monitor scheme in [13], so that a control center can monitor both voltage dynamics and rotor angle dynamics.

References

[1] Falliere N, Murchu LO, Chien E (2011) W32.stuxnet dossier. Symantec, Cupertino
[2] Roadmap to secure control systems in the energy sector. http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/roadmap.pdf#search='Roadmap+to+Secure+Control+Systems+in+the+Energy+Sector'
[3] Standards. http://www.nerc.com/pa/stand/Pages/default.aspx
[4] Cleveland F (2006) IEC TC57 security standards for the power system's information infrastructure—Beyond simple encryption. In: Proceedings of the 2005/2006 IEEE PES transmission and distribution conference and exhibition, Dallas, 21–24 May 2006, pp 1079–1087
[5] Sheldon F, Batsell S, Prowell S et al (2005) Control systems cybersecurity awareness. United States Computer Emergency Readiness Team (US-CERT), Washington, DC
[6] Depoy J, Phelan J, Sholander P et al (2005) Risk assessment for physical and cyber-attacks on critical infrastructures. In: Proceedings of the IEEE military communications conference (MILCOM'05), vol 3, Atlantic City, 17–20 Oct 2005, pp 1961–1969
[7] Ten CW, Maninaran G, Liu CC (2010) Cybersecurity for critical infrastructures: attack and defense modeling. IEEE Trans Syst Man Cybern A 40(4):853–865
[8] Ten CW, Liu CC, Maninaran G (2008) Vulnerability assessment of cybersecurity for SCADA systems. IEEE Trans Power Syst 23(4):1836–1846
[9] Sheyner OM (2004) Scenario graphs and attack graphs. Ph D Thesis, Carnegie Mellon University, Pittsburgh
[10] Pecora LM, Carroll TL (1990) Synchronization in chaotic systems. Phys Rev Lett 64:821–824
[11] Pecora LM, Carroll TL (1991) Driving systems with chaotic signals. Phys Rev A 44(4):2374–2385
[12] Vilela-Mendes R (1998) Conditional exponents, entropies and a measure of dynamical self-organization. Phys Rev A 248(2/3/4):167–171
[13] Yan J, Liu CC, Vaidya U (2011) PMU-based monitoring of rotor angle dynamics. IEEE Trans Power Syst 26(4):2125–2133
[14] Yan J, Liu CC, Govindarasu M (2011) Cyber intrusion of wind farm SCADA system and its impact analysis. In: Proceedings of the 2011 IEEE PES power systems conference and exposition, Phoenix, 20–23 Mar 2011, 6 pp
[15] IEEE 10 generator 39 bus system. http://sys.elec.kitami-it.ac.jp/ueda/demo/WebPF/39-New-England.pdf

Jie YAN received his Ph.D. degree from Iowa State University. He is currently a market engineer in MISO.

Manimaran GOVINDARASU received the Ph.D. degree in computer science and engineering from the Indian Institute of Technology, Madras, India, in 1998. He is currently an associate professor with the Department of Electrical and Computer Engineering, Iowa State University (ISU). His research expertise is in the areas of resource management in real-time systems and networks, overlay networks, network security, and their applications to critical infrastructures such as the electric grid. He has published over 100 peer-reviewed research publications. He is the coauthor of the book

entitled Resource Management in Real-Time Systems and Networks (MIT Press, 2001). He received the Young Engineering Research Faculty Award at ISU in 2003. He has given tutorials on Internet infrastructure security in conferences, such as the IEEE Infocom 2004 and IEEE ComSoc Tutorials Now (2004), and served as Workshop Cochair, Symposium Cochair, and Session Chair on many occasions.

Chen-Ching LIU received his Ph.D. degree from the University of California, Berkeley. He is currently the Boeing distinguished professor of the School of Electrical Engineering and Computer Science at Washington State University, and a professor of power systems at University College Dublin, Ireland as well. During 2006 to 2008, he was palmer chair professor of electrical and computer engineering at Iowa State University. Prior to joining ISU, he was a professor of electrical engineering at the University of Washington, Seattle. He received the IEEE PES Outstanding Power Engineering Educator Award in 2004. He served as Chair of the Technical Committee on Power System Analysis, Computing, and Economics, IEEE Power and Energy Society, during 2005 to 2006.

Ming NI received his B.S. and Ph.D. degrees in electrical engineering in 1991 and 1996 respectively, from Southeast University of China. He is now the special expert in NARI Technology Co. Ltd. His main research interest include mutual-impact between ICT and power system. Before joining Technology Co. Ltd. in 2012, he was the manager of economic studies in MISO, Minnesota, USA.

Umesh VAIDYA received the Ph.D. degree in mechanical engineering from the University of California at Santa Barbara, Santa Barbara, in 2004. He was a research engineer at the United Technologies Research Center (UTRC), East Hartford, CT. He is currently an assistant professor in the Department of Electrical and Computer Engineering, Iowa State University. His research interests include dynamical systems and control theory, in particular analysis and control of nonequilibrium behavior in nonlinear systems and application of ergodic theory methods to control problems.