Frontiers of Information Technology & Electronic Engineering
www.zju.edu.cn/jzus; engineering.cae.cn; www.springerlink.com
ISSN 2095-9184 (print); ISSN 2095-9230 (online)
E-mail: jzus@zju.edu.cn

On modeling of electrical cyber-physical systems considering cyber security*

Yi-nan WANG[†1], Zhi-yun LIN[†‡1], Xiao LIANG[2], Wen-yuan XU[1], Qiang YANG[1], Gang-feng YAN[1]

([1]*College of Electrical Engineering, Zhejiang University, Hangzhou 310027, China*)

([2]*Smart Grid Research Institute, State Grid, Beijing 102209, China*)

[†]E-mail: 11410065@zju.edu.cn; linz@zju.edu.cn

Received Dec. 13, 2015; Revision accepted Apr. 10, 2016; Crosschecked Apr. 19, 2016

Abstract: This paper establishes a new framework for modeling electrical cyber-physical systems (ECPSs), integrating both power grids and communication networks. To model the communication network associated with a power transmission grid, we use a mesh network that considers the features of power transmission grids such as high-voltage levels, long-transmission distances, and equal importance of each node. Moreover, bidirectional links including data uploading channels and command downloading channels are assumed to connect every node in the communication network and a corresponding physical node in the transmission grid. Based on this model, the fragility of an ECPS is analyzed under various cyber attacks including denial-of-service (DoS) attacks, replay attacks, and false data injection attacks. Control strategies such as load shedding and relay protection are also verified using this model against these attacks.

Key words: Cyber-physical systems, Cyber attacks, Cascading failure analysis, Smart grid
http://dx.doi.org/10.1631/FITEE.1500446 **CLC number:** TM711; TP11

1 Introduction

A smart grid is a modern electrical grid with improved reliability, efficiency, and safety (Gungor *et al.*, 2011). It integrates advanced control and modern communication technologies in power systems. A double-layer model is a natural way to abstract a smart grid with a communication network on top of a power network. However, strong interdependency between the communication network and the power network may lead to new threats on electrical cyber-physical systems (ECPSs) (Chen *et al.*, 2012; Morris and Barthelemy, 2013; Schneider *et al.*, 2013; Shin *et al.*, 2014). Intruders are able to change normal power operations via cheating commands through communication networks. Also, catastrophic cascade of failures in ECPSs may be triggered by a failure of a small fraction of nodes in only one network. To analyze possible cascading failures due to cyber attacks, it is extremely important to find proper models for ECPSs. On this issue, research efforts have been undertaken along several different approaches.

One approach adopts complex network modeling for both communication networks and power networks, and analyzes cascading failures from the perspective of topology interdependency. Buldyrev *et al.* (2010) considered an ECPS model by assuming that the communication network is a scale-free network. Huang *et al.* (2011) further studied the ECPS model proposed in Buldyrev *et al.* (2010) from

‡ Corresponding author

* Project supported by the National Basic Research Program (863) of China (No. 2015AA05002), the National Natural Science Foundation of China (No. 61471328), and the Science and Technology Project of State Grid, China (No. XXB17201400056)

ORCID: Zhi-yun LIN, http://orcid.org/0000-0002-5523-4467

the robustness viewpoint. In Buldyrev *et al.* (2011), identical degrees of mutually dependent nodes were used to model the communication network. Parandehgheibi *et al.* (2014) used a DC power model to describe power grids, while communication networks were just abstracted as a complete graph. Yang *et al.* (2011) pointed out that for communication infrastructures in power distribution networks, telecommunication networks have two representative topologies. Although communication networks in different topologies can influence the robustness of ECPSs differently, there is no unified framework to reflect topological characteristics of both power grids and communication networks. Therefore, it is necessary to find a reasonable model for the communication networks in ECPSs by considering the characteristics of power grids.

Another approach analyzes cascading failures on interdependent relationships of ECPSs caused by coupling communication networks. Shao *et al.* (2011) described the relationships with multiple support-dependence relations. Hu *et al.* (2011) took into account the one-way links between the two networks. Parshani *et al.* (2010) modified the relations by reducing the coupling strength of two networks. The disadvantage is that they neglected the characteristics that different types of transmitted information may influence ECPSs differently. Parandehgheibi *et al.* (2014) dealt with the relationship between communication networks and power grids with the assumption that communication nodes consume power from the power grids for their operations. However, in transmission grids, the power that the communication nodes need is received from uninterrupted power supply (UPS), which is divided from the power grid and has a higher security level. So, it is important to establish a unified framework to clearly describe the interdependent relationship between power grids and communication networks.

The third approach shifts the study of interdependent relationships into studying control strategies to ensure stability and cyber security to stabilize. Wei *et al.* (2014) considered ECPSs as multi-agent dynamic systems, and proposed a flocking-based paradigm for security control. The authors considered physical characteristics of generators by using a distributed coordinated control strategy. However, few nodes were contained, which does not fit for analyzing large-scale transmission grids. Chen *et al.* (2012) modeled a framework by fully considering the characteristics of ECPSs, and introduced a two-player zero-sum game between the adversary and the defender to evaluate the performance of defense mechanisms with different network configurations. The issue is that such a method cannot reflect the difference in attack types and attack points. Teixeira *et al.* (2015a; 2015b) systematically summarized various cyber attack scenarios, and described in detail attack policies, attack performance, and required model knowledge, disclosure, and disruption. However, these studies do not associate secure control with large-scale communication networks, and the dependency of ECPSs is unclear. As we have discussed previously, control strategies and the framework of ECPSs should be combined together to qualitatively analyze cascading failures and cyber security.

The key technical contributions made in this study can be summarized as follows. First, we establish a new framework for ECPSs with a power grid coupled with a communication network. Based on the characteristics of high-voltage levels, long-transmission distances, and the importance of each node in transmission grids, the communication network is modeled as a meshed topology with each node associated with a physical node in transmission grids. Second, we qualitatively apply the load shedding and relay protection control schemes (Wang, 2012) in our framework and the control decisions are made automatically by control centers according to real-time information. Third, we provide rigorous analysis for the propagation of cascading failures in ECPSs combined with modern control in entirety. To the best of our knowledge, this work is the first attempt to incorporate several cyber attack scenarios into relevant conventional relay protection policies for cascading failure analysis. Through numerical simulations the effectiveness of relay protection control and the fragility of ECPSs under cyber attacks are demonstrated.

Compared with existing solutions, our proposed framework has two advantages. First, this framework has portability. It can be used in any power system. Given a power grid, we can design communication networks and relationships between two networks to analytically and numerically analyze the

mechanism of cascading failures. In contrast, others abstract a real communication network for specific analysis or count the total number of nodes in a power grid and generate a large-scale communication network with power law distributions. The former is of heavy work because we need to acquire the topology of a communication network and repeat the work when the situation is changed. The latter is too general to capture the characteristics mentioned above. In our framework, the related communication network can be generated automatically and reflects the special characteristics comprehensively. Second, we describe the relationship between power systems and communication networks by distinguishing different types of information transmission and visualizing it into four types of information channels, which contributes to the exploration for the mechanisms of avoiding cascading failures in ECPSs.

2 Framework of ECPSs

According to Yang *et al.* (2011) and Wang (2012), power transmission grids have two characteristics. One is that the voltage level is high and the transmission distances are long. The other is that every component in the transmission grid plays a key role so that each power node is equipped with a router and each line is equipped with a breaker. These routers receive information from the power nodes and relay it to the control center through gateways. The control center makes wide-area control decisions and sends them back to the routers located at power nodes. Then the decisions are executed by the prime motors, load tripping devices, or the breakers. There are several communication devices such as supervisory control and data acquisition (SCADA) and phasor measurement unit (PMU) systems that transmit information to the regional control center that is responsible for making control decisions.

To capture the characteristics of power transmission grids above, we establish a new framework for ECPSs and design the relationships between power grids and communication networks. Our proposed framework for ECPSs has a communication network in meshed topology atop a power grid. Each communication node is associated with a power node in the transmission grid. There is also an extra control center node which is connected to all the communication nodes in an area.

Previous studies (Shao *et al.*, 2011; Parandehgheibi *et al.*, 2014) tried to describe the relationships in graph theories by multiple support-dependence relations or considering power supply and consumption relations. However, they neglected the characteristics that various types of transmitted information influence ECPSs differently. In our framework for ECPSs, we distinguish various types of information transmission to describe the relationships of ECPSs so that the interdependency of ECPSs in our design is visible and specific. The idea of modeling a power grid by the graph theory (Parandehgheibi *et al.*, 2014) is adopted in Section 2.1. The new framework for ECPSs and a generation method for the relevant communication network based on a given power grid are introduced in Section 2.2.

2.1 Modeling a power grid

According to Parandehgheibi *et al.* (2014), a power grid can be modeled as a graph $G_{\mathrm{P}} = (V_{\mathrm{P}}, E_{\mathrm{P}})$, where V_{P} and E_{P} are the sets of power nodes and lines, respectively. Three classic types of power nodes are considered: generator nodes ($V_{\mathrm{P}}^{\mathrm{G}}$), load nodes ($V_{\mathrm{P}}^{\mathrm{L}}$), and substation nodes ($V_{\mathrm{P}}^{\mathrm{S}}$). Generators generate power and transmit it to the load nodes that consume power through the power lines, while the substation nodes that neither generate nor consume power act as the role of regulating voltages. The flows in power lines are driven by Kirchhoff's laws. The DC power flow model (Stott *et al.*, 2009) is used to analyze the behaviors of a power grid.

Let $\boldsymbol{p}$ be a $|V_{\mathrm{P}}|$-dimensional vector ('$|\cdot|$' represents the cardinality of the set) so that p_k denotes the power injection at a power node $k \in V_{\mathrm{P}}$. Let $\boldsymbol{A} \in \mathbb{R}^{|V_{\mathrm{P}}|\times|E_{\mathrm{P}}|}$ be the incidence matrix where $A(i,j) = 1$ if link j starts from node i, $A(i,j) = -1$ if link j ends in node i, and $A(i,j) = 0$ if link j does not go through node i. Matrix $\boldsymbol{A}$ reflects the topology of the power grid, and switching on or off a line can change the entry or dimension of $\boldsymbol{A}$. Let $\boldsymbol{X} \in \mathbb{R}^{|E_{\mathrm{P}}|\times|E_{\mathrm{P}}|}$ be the reactance diagonal matrix associated to the power grid, where $X(i,i)$ denotes the reactance of the ith power line. Moreover, let $\boldsymbol{f} \in \mathbb{R}^{|E_{\mathrm{P}}|}$ be the vector of power flows in transmission lines and $\boldsymbol{\theta} \in \mathbb{R}^{|V_{\mathrm{P}}|}$ the phases at all power

nodes. Then a DC power flow can be modeled as

$$\boldsymbol{A}\boldsymbol{f} = \boldsymbol{p}, \tag{1}$$

$$\boldsymbol{A}^{\mathrm{T}}\boldsymbol{\theta} = \boldsymbol{X}\boldsymbol{f}. \tag{2}$$

Eq. (1) is used to calculate the power in each node, while Eq. (2) is used to model the power flow in every line. If the power injection has changed, the power flow in every line will be redistributed, and vice versa.

2.2 Design of a framework for ECPSs

In the graph theory, a communication network can be described as a graph $G_{\mathrm{C}} = (V_{\mathrm{C}}, E_{\mathrm{C}})$, where V_{C} and E_{C} are the sets of communication nodes and lines, respectively. Three traditional types of communication nodes (Wang, 2012) are included: (1) sensors on breakers (breakers that are responsible for local overload protection, which can switch off the fault line immediately), (2) control center that is responsible for making control decision, and (3) routers that are responsible for transmission information (uploading messages from power grids and downloading messages from communication networks). Modern control strategies such as automatic generation control (AGC), automatic voltage control (AVC), and automatic stability control (ASC) are decided by the control center which gathers information through routers and pushes commands to sensors and actuators on breakers. Communication devices such as SCADA and PMU also use routers to transmit information.

Based on the proposed framework, we can describe the relationship between power grids and communication networks. First, we distinguish the different channels based on the types of transmitted information. According to our design on communication networks, sensors on beakers, routers, and control centers have their own channels to transmit messages or commands. Second, in our design, the interdependency of two networks is concrete; i.e., a node in power grids can function even if it is not connected to any node in communication networks (called an 'isolated physical node'). The isolated physical node is out of control and could be caused by the redistribution of the power grid, if the control center changes the control strategy but the information cannot be transmitted to the node. However, a node in communication networks can function only if the communication node belongs to a connected cyber network. The connectivity of a node in communication networks is more important than a node in power grids, and thus we focus on the faults of communication that are caused by cyber attacks on information channels instead of the support link connecting to power grids.

Given a model of power grids in Section 2.1, Fig. 1 shows the design of an ECPS and its relevant interdependent relationship. There are two planes in the figure: the communication network plane and the power grid plane. We define channel 1 as the channel through which information is uploaded from power nodes to routers in the communication network and finally to the control center (e.g., C-(1) in Fig. 1), channel 2 as the channel through which commands are downloaded from the control center directly to power nodes (e.g., C-(2) in Fig. 1), and channel 3 as the channel through which commands are downloaded from the control center directly to breakers in the power line (e.g., C-(3) in Fig. 1). There are also

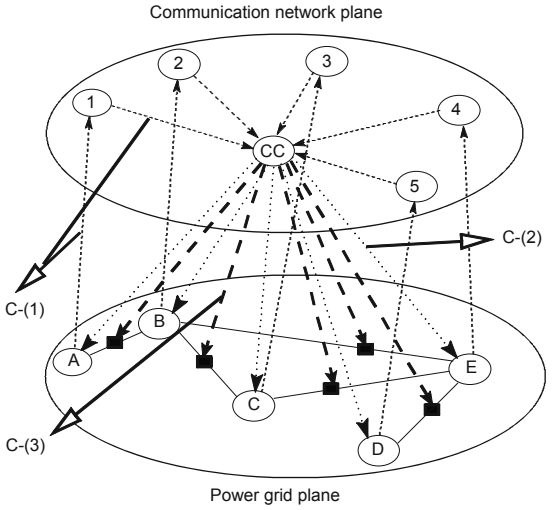

Fig. 1 Interdependent relationships in a regional electrical cyber-physical system (ECPS). Nodes A–E stand for five physical nodes in the power grid plane. They can be generators, loads, or substations. The lines among nodes A–E are transmission lines where power flows exist. The solid black rectangles on the power lines are breakers. The communication network plane contains a control center (CC) and five router nodes (1–5) which are associated with the power nodes (A–E) respectively. Dashed lines: channel 1 (e.g., C-(1)); dotted lines: channel 2 (e.g., C-(2)); bold dashed lines: channel 3 (e.g., C-(3)). Arrows represent the directions of information flows

local channels through which a power line controls a breaker to cut off the fault line and they are not displayed in Fig. 1.

Fig. 1 describes a regional framework for ECPSs, which can be considered as a centralized control framework. Actually, the real scale of power transmission grids is large. The power transmission grids are divided into several regions owing to spatial distance, while they are still physically interconnected. We define channel 4 as the channel through which regional control centers connect with each other (e.g., C-(4) in Fig. 2). Fig. 2 is the macroscopic model of a large-scale ECPS with n regional control centers. It is a decentralized control model.

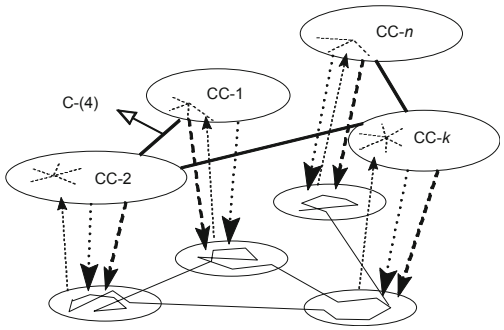

Fig. 2 Framework for a large-scale ECPS. Bold solid lines: channel 4 (e.g., C-(4)); CC-i ($i = 1, 2, \ldots, n$): regional control center i

Based on our proposed framework for ECPSs, Tables 1–3 compare the new model of ECPSs with existing models. Tables 1 and 2 separately focus on the modeling approaches of power grids and communication networks. Our model uses a more general and typical way for node classification and obeys Kirchhoff's laws and the mechanism of information transmission. Table 3 shows the differences of modeling the interdependent relationships between power grids and communication networks from three perspectives: which part of the ECPS is influenced by the relationship (actuator), the function of the actuator (function), and whether the influence has a direction (directional). Compared with other studies which model interdependency mainly on single or multiple support-dependence relations with the assumption that a node in one network can function only if at least a single support link connects it to a functional node in the other network, our model distinguishes different channels with the types of information transmissions. We can understand the complex interdependency in a real ECPS in this way.

In the next section, we will add current control schemes and attack scenarios to our proposed framework. Consequences of the system acting on information channels 1–3 through the design of interdependent relationships are also studied. Channel 4 is thought to have the highest security level and the capacity is high enough, so that the probability of faults on channel 4 is negligible. In this study, we assume that channel 4 is reliable and fault scenarios do not occur on channel 4.

3 Control schemes and attack scenarios

Previous study (Wang, 2012) has proposed a load shedding control scheme added to the relay protection to mitigate failures inside the single power grid. Generally, the control scheme is executed manually after the failures. The traditional relay protection control strategy uses only neighboring information to cut off a fault line or switch it on if the fault is repaired. Since other models do not distinguish different information channels, and control schemes may change with channels, it is difficult to study the influence on the fault in information transmissions. We overcome these difficulties in our established framework by differentiating information channels.

We qualitatively extend the shedding control scheme to our designed framework for ECPSs, and the shedding control decisions are made automatically by control centers according to the real-time fault information uploaded through channel 1 in situation I. When a failure occurs in power grids, which is usually caused by the short circuit and leads to a transmission line overload (Bao *et al.*, 2009), the control center will make correct decisions to minimize the loss and stabilize the system as soon as possible. We have examined various types of cyber attacks (Teixeira *et al.*, 2015b) targeted at the information transmission mentioned in Section 2, to study the consequence of attacks and attack points. If the information transmission channels are broken or attacked by hackers, the actuator may receive fake commands and the control center may receive fault information. As a consequence, the ECPS may suffer

Table 1 Differences of modeling approaches on power grids

ECPS model	Generation type	Classification of nodes	Directional	Mechanism
Our approach	Realistic power grid	Substation, generator, and load	Yes	Kirchhoff's law
Buldyrev *et al.* (2010) & Schneider *et al.* (2013)	Complex network	None	No	Generation function
Shao *et al.* (2011)	Complex network	None	No	Generation function
Parandehgheibi *et al.* (2014)	Realistic power grid	Substation, generator, and load	Yes	Kirchhoff's law
Wei *et al.* (2014)	Realistic power grid	Generator and load	Yes	Kirchhoff's law

Table 2 Differences of modeling approaches on communication networks

ECPS model	Generation type	Classification of nodes	Directional	Mechanism
Our approach	Generate automatically	Sensors on breakers, router, and control center	Yes	Information transmission
Buldyrev *et al.* (2010) & Schneider *et al.* (2013)	Complex network	Nodes (SCADA/PMU)	No	Generation function
Shao *et al.* (2011)	Complex network	Nodes (SCADA/PMU)	No	Generation function
Parandehgheibi *et al.* (2014)	Complex network	Router and control center	Not connected	No
Wei *et al.* (2014)	Complex network	Nodes (PMU)	No	Information exchange

Table 3 Differences of modeling approaches on interdependent relationships

ECPS model	Actuator		Function		Directional	
	Coupling 1	Coupling 2	Coupling 1	Coupling 2	Coupling 1	Coupling 2
Our approach	Classified (node/line)	Classified (node/line)	Monitoring, protection, and control	Isolated physical node	Yes	Yes
Buldyrev *et al.* (2010) & Schneider *et al.* (2013)	Not classified	Not classified	Dependent	Dependent	No	No
Shao *et al.* (2011)	Not classified	Not classified	Control	Dependent	Yes	Yes
Parandehgheibi *et al.* (2014)	Not classified	Not classified	Control	Power supply	Yes	Yes
Wei *et al.* (2014)	Classified	Classified	Control	Frequency control	Yes	Yes

Coupling 1: from communication networks to power grids; coupling 2: from power grids to communication networks

from a critical failure. The combination of ECPSs under different cyber attack scenarios at the topological layer and control layer is described in situations II and III.

Much work on computer attacks and security has focused on data and information technology (IT) services (Bishop, 2002). In this study, we consider three cyber attacks in ECPSs: denial-of-service (DoS) attacks, replay attacks, and false data injection attacks. According to Teixeira *et al.* (2015b), DoS attacks aim at preventing actuating and sensory data from reaching their respective destinations and result in the absence of data. Replay attacks transmit the recorded data gathered before. False data injection attacks aim to inject a constant bias in the system through information channels (Liu *et al.*, 2011). DoS attacks can be applied on a local channel or channels 1–3, and delay the real information transmission. Replay attacks can be applied on channels 1–3 and replace a sequence of data or commands.

False data injection attacks can be applied on a local channel or channels 1 and 2, and thus data can be tampered deliberately, which may do great harm to the system.

Let $v=(a,b)$ represent the vth line along which power flow goes from node a to node b via edge $v\in E_{\mathrm{P}}$. First, we make three assumptions for the ECPS model:

(A1) Each transmission line v has a maximum power capacity limit ($f_{ab}^{\max}$);

(A2) Each generator has a maximum allowed output power;

(A3) The power can be balanced after each control strategy owing to the balance node.

We define three functions to simplify the description.

(1) Function $\boldsymbol{F}_v$ is the transforming function that switches off line v, and it is defined from $\mathbb{R}^{m\times n}$ to $\mathbb{R}^{m\times n}$ such that

$$F_v(\boldsymbol{H})(i,j)=\begin{cases}0, & j=v,\\ H(i,j), & \text{otherwise},\end{cases}$$

where $m,n\in\mathbb{N}_+$ and $\boldsymbol{H}\in\mathbb{R}^{m\times n}$.

(2) Function $\boldsymbol{G}_v$ is the transforming function that switches off line v, and it is defined from $\mathbb{R}^{m\times n}$ to $\mathbb{R}^{m\times n}$ such that

$$G_v(\boldsymbol{H})(i,j)=\begin{cases}1, & i=a,\ j=v,\\ -1, & i=b,\ j=v,\\ H(i,j), & \text{otherwise},\end{cases}$$

where $m,n\in\mathbb{N}_+$ and $\boldsymbol{H}\in\mathbb{R}^{m\times n}$.

(3) Function $\boldsymbol{h}$ is the control strategy function, and it is defined from $\mathbb{R}^{|V_{\mathrm{P}}|}$ to $\mathbb{R}^{|V_{\mathrm{P}}|}$ as

$$\boldsymbol{h}=[\boldsymbol{h}^{\mathrm{G}}\ \ \boldsymbol{h}^{\mathrm{L}}\ \ \boldsymbol{h}^{\mathrm{S}}],$$

with $h_k=[-p_{k\max},\ +p_{k\max}]$ being an element of $\boldsymbol{h}$, where $p_{k\max}$ is the maximum power capacity of node $k\in V_{\mathrm{P}}$ in a power grid, and $\boldsymbol{h}^{\mathrm{G}}$, $\boldsymbol{h}^{\mathrm{L}}$, $\boldsymbol{h}^{\mathrm{S}}$ are the subsets of $\boldsymbol{h}$.

Define the power injected into a node to be positive, and the power outflew a node to be negative. For a set of generator nodes ($V_{\mathrm{P}}^{\mathrm{G}}$), load nodes ($V_{\mathrm{P}}^{\mathrm{L}}$), and substation nodes ($V_{\mathrm{P}}^{\mathrm{S}}$), we have $p_k^{\mathrm{G}}>0$, $p_k^{\mathrm{L}}<0$, and $p_k^{\mathrm{S}}=0$, respectively. The maximum capacities may be different owing to the different types of nodes. For generator nodes ($V_{\mathrm{P}}^{\mathrm{G}}$), load nodes ($V_{\mathrm{P}}^{\mathrm{L}}$), and substation nodes ($V_{\mathrm{P}}^{\mathrm{S}}$), we have $h_k^{\mathrm{G}}\in[-p_{k\max},+p_{k\max}]$, $h_k^{\mathrm{L}}\in[0,+p_{k\max}]$, and $h_k^{\mathrm{S}}=0$, respectively.

In this study, function $\boldsymbol{F}_v$ is used to represent the change of the topology of power grids after a breaker cuts off a line. Correspondingly, function $\boldsymbol{G}_v$ is used to represent the change of the topology of power grids after a breaker switches on a line, while function $\boldsymbol{h}$ is a continuous control vector applied to electrical power nodes.

Based on the aforementioned assumptions and definitions, we apply the load shedding and relay protection control schemes to our designed communication networks. Due to the special relationships brought out by the design, the relay protection control can be controlled by a wide-area control center through channel 3. Similarly, the load shedding policy uses global information to make decisions through channels 1 and 2. Here we formulate three typical control instructions in a process of fault handling based on the DC flow (Eqs. (1) and (2)). Table 4 shows the relationships among control instructions, commands, information transmission channels, and protection actuators, when a fault occurs (i.e., line $v=(i,j)$ overloads).

In Table 4, note that in type 1, the breaker uses only local information to make decisions. In this action, there is no information exchanged between the physical and cyber systems. In type 3, however, the action of a breaker to switch on is decided by the control center in the communication network, and the instruction is transmitted through channel 3. In type 2, if the grid is overloaded, it is required to decrease the amount of power at regional loads or generators. The DC power flow will be resolved after every action.

Next, we will describe three situations to show

Table 4 Three typical control instructions

Type	Instruction	Command	Actuator	Channel
1	Cut off the line	$\boldsymbol{F}_v(\boldsymbol{A})$	Breaker	Local channel
2	Shed loads	$\boldsymbol{p}=\boldsymbol{p}+\boldsymbol{h}$	Generator and load	Channels 1 and 2
3	Switch on the line	$\boldsymbol{F}_v(\boldsymbol{A})$	Breaker	Channels 1 and 3

how the control strategies are extended to the proposed framework. Consequences caused by the strategies are also discussed. In situations II and III, we focus on several cyber attacks.

3.1 Situation I

Background: The vth line $v=(i,j)$ overloads at discrete time k, which causes $f_{ij}>f_{ij}^{\max}$.

Control strategy:

(1) $\boldsymbol{A}[k+1]=\boldsymbol{F}_v(\boldsymbol{A}[k])$,

(2) $\boldsymbol{h}^{\mathrm{G}}[k+2]=-0.1\boldsymbol{p}^{\mathrm{G}}[k+1]$ or $\boldsymbol{h}^{\mathrm{L}}[k+2]=-0.1\boldsymbol{p}^{\mathrm{L}}[k+1]$,

(3) $\boldsymbol{p}[k+3]=\boldsymbol{p}[k+2]+\boldsymbol{h}[k+2]$,

(4) $\boldsymbol{A}[k+4]=\boldsymbol{G}_v(\boldsymbol{A}[k+1])$.

Explanation: To understand the control strategy above, we define the following loss function:

$$J=\sum_{i\in V_{\mathrm{P}}^{\mathrm{G}}}\left|p_i^{\mathrm{G}_{\mathrm{new}}}-p_i^{\mathrm{G}_{\mathrm{old}}}\right|+\lambda\sum_{j\in V_{\mathrm{P}}^{\mathrm{L}}}\left|p_j^{\mathrm{L}_{\mathrm{new}}}-p_j^{\mathrm{L}_{\mathrm{old}}}\right|, \quad (3)$$

where p_i^{G} and p_j^{L} represent the power injections of generator node i and load node j, respectively. Note that notations 'old' and 'new' represent the power injections at the corresponding nodes before and after applying the control strategy, respectively. Moreover, define λ as a constant larger than 1 because load shedding is more expensive than generation shift (Dobson *et al.*, 2001).

A complete control procedure can be divided into four steps. In the first step, the breaker finds the fault and cuts off the line immediately by local control. Then in the second step, the fault information is transmitted through channel 1 to the control center. The control center analyzes the information and makes decision. Whether generators or loads should shed loads depends on the minimization of J caused by this control decision. The parameter 0.1 (in the control strategy in situation I) has been decided in Wang (2012). In the third step, the instruction is downloaded to the power nodes through channel 2. Lastly, the center controls the line breaker to switch on through channel 3. After the four steps, a process is completed and the power flow redistributes.

3.2 Situation II

Background: The vth line $v=(i,j)$ overloads at discrete time k, which causes $f_{ij}>f_{ij}^{\max}$. At time $k+1$, two kinds of cyber attacks (DoS attack and replay attack) respectively disturb the information channels of the ECPS. In this study, we assume that during the DoS attack, the grid will continue to use the latest renewed data if no update is recorded. In replay attacks, the channel will use the recorded data at time w ($w<k$).

Attack policy: Tables 5 and 6 show the differences of channels being attacked and the false control commands caused by the DoS attacks and replay attacks, respectively. All processes start when line $v=(i,j)$ overloads.

Table 5 An ECPS under the DoS attack

Attack on	False command	Actuator
Local channel	$(1)'\ \boldsymbol{A}[k+1]=\boldsymbol{A}[k]$	Breaker
Channel 1	$(2)'\ \boldsymbol{h}[k+2]=\boldsymbol{h}[k+1]$	–
Channel 2	$(3)'\ \boldsymbol{p}[k+3]=\boldsymbol{p}[k+2]+\boldsymbol{h}[k+1]$	Generator and load
Channel 3	$(4)'\ \boldsymbol{A}[k+4]=\boldsymbol{A}[k+3]$	Breaker

Table 6 An ECPS under the replay attack

Attack on	False command	Actuator
Channel 1	$(2)''\ \boldsymbol{h}[k+2]=\boldsymbol{h}[w]$	–
Channel 2	$(3)''\ \boldsymbol{p}[k+3]=\boldsymbol{p}[k+2]+\boldsymbol{h}[w]$	Generator and load
Channel 3	$(4)''\ \boldsymbol{A}[k+4]=\boldsymbol{A}[w]$	Breaker

Explanation: Tables 5 and 6 list the influenced control commands caused by the attack compared with the complete control strategy in situation I. Each row describes an independent attack. Under each attack, the ECPS will experience the four steps of the control strategy in situation I, while part of the commands may be disturbed due to the attack.

Particularly, for DoS attacks, when line $v=(i,j)$ overloads, if the attack occurs on the local control, the breaker remains switched on. If the attack prevents the fault information from being uploaded to the control (channel 2), the control center will not receive the warning and do nothing for the power system. The actuators will not act due to the attack on channels 2 and 3. All these false commands can lead to a large-scale cascading failure. Similarly, for replay attacks in the same scenario, the attack can be launched on channels 1–3.

In our analyses, we combine attacks with the control of ECPSs. Note that whether the two

aforementioned attacks can cause cascading failures in ECPSs or not depends on the control strategy. However, if the control strategies at times w and $k+1$ are the same, then the consequences of the two attacks on channels 1 and 2 will be the same.

3.3 Situation III

Background: At time k, the ECPS operates normally. At time $k+1$, the false data injection attack (Teixeira *et al.*, 2015b) will disturb the information channels of the ECPS. The purpose is to make the vth line $v=(i,j)$ overload, which causes $f_{ij}>f_{ij}^{\max}$.

Attack policy: Table 7 shows the differences of channels being attacked and the false control commands caused by the injection attack ($\boldsymbol{h}^{\text{active}}$ represents the deliberately injected constant bias).

Table 7 An ECPS under the false data injection attack

Attack on	False command	Actuator
Local channel	$(1)''\ \boldsymbol{A}[k+1]=\boldsymbol{F}_v(\boldsymbol{A}[k])$	Breaker
Channel 1	$(2)''\ \boldsymbol{h}[k+2]=\boldsymbol{h}^{\text{active}}$	–
Channel 2	$(3)''\ \boldsymbol{p}[k+3]=\boldsymbol{p}[k+2]+\boldsymbol{h}^{\text{active}}$	Generator and load

Explanation: Table 7 lists the influenced control commands caused by the injection attack compared with the complete control strategy in situation I.

Note that for replay attacks on channels 1–3, the recorded data at time w injected to the ECPS may not solve the current fault but may mitigate or worsen the situation. However, attackers do not know the degree of influence. As for attackers who apply the replay attacks, they have limited resources of the framework for ECPSs, so the time w is chosen randomly or based on the eavesdropping equipment. Here, we discuss two situations:

1. If at time w, the power system operates at an optimal state, then there is no need to apply any control measure. Thus, $\boldsymbol{h}[w]=\boldsymbol{0}$. Compared with the control strategy in situation I (step (2)), replay attacks can worsen the situation by 10% of control measure.

2. If at time w, the power system needs to shed off 10% of the generations (or demands) so that the system can move to an optimal state, then $\boldsymbol{h}[w]=-0.1\boldsymbol{p}^{\text{G}}[w-1]$ (or $\boldsymbol{h}[w]=-0.1\boldsymbol{p}^{\text{D}}[w-1]$). Compared with the control strategy in situation I (step (2)), replay attacks can mitigate the situation.

So, it can be seen that replay attacks can disturb the system only by probability. As for false data injection attacks, $\boldsymbol{h}^{\text{active}}$ can be carefully designed with a 'desired' consequence. Attackers know the framework for ECPSs, so they can inject false data to the information channels to disturb the normal operations of ECPSs. Attackers can worsen the situation by 50% or more of the control measure by tampering $\boldsymbol{h}^{\text{active}}$. If an attacker wants to imply a fearful attack through replay attacks, he/she needs to acquire more information about the system, which increases the difficulty of attack. In other words, the false data injection attack can cause a larger-scale failure easily.

4 Mechanism of cascading failure propagation

In this section, we describe the mechanism of cascading failure propagation based on our framework for ECPSs. The control scheme and cyber security detection introduced in Section 3 are included in the propagation. An initial outage of a physical component changes the balance of the power flow distribution over the grid and causes a redistribution of the power flow over the network. This dynamic response of the system due to the triggering event might overload other parts in the physical network and change the current control policies in the control center in the communication network. In case of isolating in power grids, the relevant routers in communication networks will be useless, which in turn disturbs the decision. Cascading failures in ECPSs continue until no more components are overloaded and the system is stable.

Generally, the process of cascading failure propagation in ECPSs will be divided into four categories: (1) cascading failure propagation in physical power systems; (2) cascading failure propagation in cyber communication networks; (3) influence of communication networks on power grids; (4) influence of power grids on communication networks.

The mechanism of cascading failure propagation in a single physical or cyber system (categories (1) and (2)) has been studied for many years. In physical power systems, one fault in the grid will cause power flows to redistribute based on Kirchhoff's laws. The

redistribution of power flows may cause other lines or nodes to be overloaded. The process will not stop until the power flow in each line is under a safe range (Baldick *et al.*, 2008). In cyber communication networks, similar failure propagation will be caused by packet loss, network delay, and service failures (Chakrabarti and Manimaran, 2002).

In this study, we aim to solve categories (3) and (4). The influence of communication networks on power grids reflects on extra power injection injected to the generators or loads through channel 2 by control strategies. Recent research has focused mainly on analyzing the stabilization of a system under one single fault or an attack. We try to use current simple strategies to study the stabilization of the system under a series of cascading failures.

In Fig. 1, if channel 1 is broken, the control center cannot receive the failure data and thus can do nothing to mitigate the cascading failures in power grids. If channel 2 or channel 3 is broken, the control commands cannot be downloaded to the actuators as well. Moreover, if several channels are broken, the control center can receive only part of the information, and the strategies will not be proper for the whole system and may worsen the situation. In turn, the faults in power grids may let breakers cut off the lines, which leads to several nodes being disconnected in entirety. The loss of several nodes and lines means the loss of relevant information transmission. The channels among these nodes and lines become useless. In this way, the cascading failures propagate through ECPSs.

Assume that the information channels have only two states: normal and abnormal. When a channel is abnormal, it means that the information cannot be transmitted through the channel. The cascading failure propagation procedure in ECPSs begins from a base load flow and follows the steps below:

(a) At time k, randomly select a transmission line $v=(i,j)$ as the initial triggering event, $f_{ij}>f_{ij}^{\max}$.

(b) At time $k+1$, examine a breaker's local control channel.

(b-1) If it is normal, trip the selected line, $\boldsymbol{A}[k+1]=\boldsymbol{F}_v(\boldsymbol{A}[k])$. Search for isolated components, if has, and update the graph topology, $G_{\mathrm{C}}^{\mathrm{update}}=(V_{\mathrm{C}}^{\mathrm{update}},E_{\mathrm{C}}^{\mathrm{update}})$.

(b-2) If it is abnormal, no action, $\boldsymbol{A}[k+1]=\boldsymbol{A}[k]$.

(c) At time $k+2$, examine channel 1.

(c-1) If it is normal, upload fault information to the control center, and make decision $\boldsymbol{h}[k+2]$.

(c-2) If it is abnormal, no fault information is uploaded, $\boldsymbol{h}[k+2]=\boldsymbol{h}[k+1]$.

(d) At time $k+3$, examine channel 2.

(d-1) If it is normal, download control instructions to the nodes, $\boldsymbol{p}[k+3]=\boldsymbol{p}[k+2]+\boldsymbol{h}[k+2]$.

(d-2) If it is abnormal, no control instructions are downloaded, $\boldsymbol{p}[k+3]=\boldsymbol{p}[k+2]$.

(e) At time $k+4$, examine channel 3.

(e-1) If it is normal, download control instructions to the breakers, $\boldsymbol{A}[k+4]=\boldsymbol{G}_v(\boldsymbol{A}[k+3])$.

(e-2) If it is abnormal, no control instructions are downloaded, $\boldsymbol{A}[k+4]=\boldsymbol{A}[k+3]$.

(f) At time $k+5$, redistribute the power flow by Eqs. (1) and (2).

(f-1) If there exists $i,j\in V_{\mathrm{P}}$ such that $f_{ij}>f_{ij}^{\max}$, then go back to step (b).

(f-2) If for every $i,j\in V_{\mathrm{P}}$ there is $f_{ij}\le f_{ij}^{\max}$, then go to step (g).

(g) Stop the procedure, record the loss, and evaluate the fault scale.

In the procedure, steps (b-2), (c-1), (d-1), and (e-1) reflect the cyber attacks on the ECPS (see Section 3 for details). As for the situation where cascading failures in ECPSs are triggered by a cyber attack, it still follows the above steps but the procedure begins at step (b-2), (c-1), (d-1), or (e-1) according to different cyber attacks.

The procedure has the following advantages. First, the proposed procedure can reflect the failure propagation of coupled networks (ECPSs). We can see the evolutionary process of how the communication network influences the power system, and vice versa. Second, adding intelligent control strategies to the mechanism of cascading failure propagation makes the analysis more complex but practical. Last, we visualize the interdependency of ECPSs by different information channels and firstly combine the cyber attacks with the analyzing mechanism.

Here we introduce an evaluation criterion for cascading failures. The fraction of nodes (δ) represents the ratio of the rest of the connected nodes after the cascading failure occurs to the whole number of the nodes in the power grid:

$$\delta=|V_{\mathrm{P}}|^{\mathrm{final}}/|V_{\mathrm{P}}|. \tag{4}$$

The system has been demonstrated to have better robustness with the value of δ close to 1 (Koç *et al.*, 2014).

5 Numerical examples and simulation results

In this section, we analyze the cascading failure and the performance of load shedding and relay protection control policies through MATLAB simulations. Our proposed framework of ECPSs has portability. Given a power grid, we can generate the relevant communication network and the relationship between two networks to analytically and numerically analyze the mechanism of cascading failures. In general, the IEEE 9-, 14-, 30-, and 39-bus systems are used to simulate physical power grids in the simulations (http://www.ee.washington.edu/research/pstca/), and the communication networks are designed according to Section 2. The IEEE 39-bus system is used to analyze the performance of ECPSs under cyber attacks owing to the large scale of nodes. The only difference is that in the 30- and 39-bus systems, we partition the power grid into three regions (Pasqualetti *et al.*, 2013), so that the control scheme and attack policy are distributed. Here we present the ECPS with the 39-bus power grid, while the others can be done in a similar way. Fig. 3 shows the partition of the IEEE 39-bus system. Note that regions 1–3 are still physically connected by transmission lines. Fig. 4 shows the macroscopic ECPS model of the IEEE 39-bus system. We abstract the physical connection through regions into one line. Each region is monitored and operated by a control center. These control centers cooperate to estimate the state and to assess the functionality of the whole ECPS. Regional control centers are interconnected through a dedicated optical network (as illustrated in Section 3).

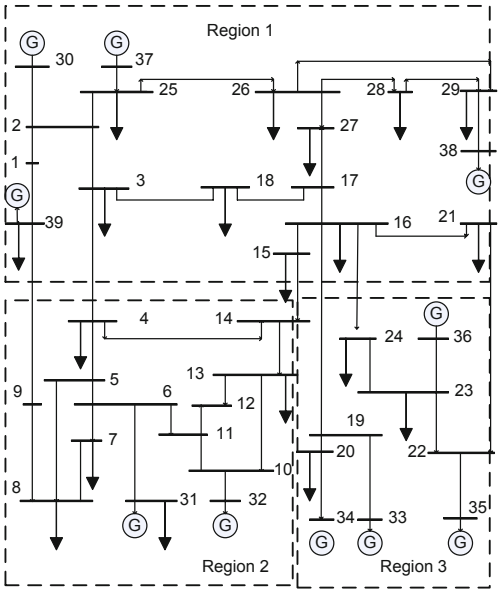

Fig. 3 Partition of the IEEE 39-bus system

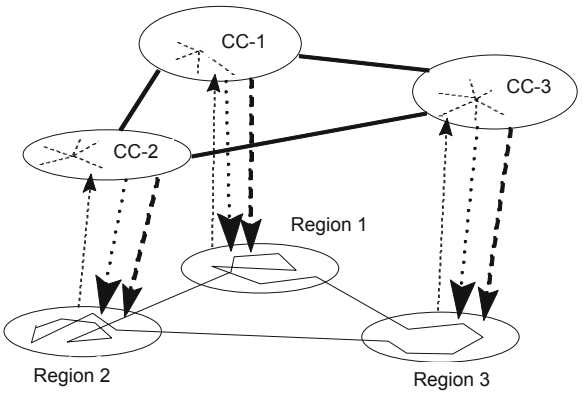

Fig. 4 ECPS of the IEEE 39-bus system. Dashed lines: channel 1 (e.g., C-(1)); dotted lines: channel 2 (e.g., C-(2)); bold dashed lines: channel 3 (e.g., C-(3)). Arrows represent the directions of information flows

5.1 Experiment settings

In the simulations, we used MATLAB to calculate the DC power flow and simulate the performance of ECPSs under cascading failures in the proposed framework.

Simulation I was conducted to analyze mainly the performance of ECPSs with an initial overload on a power line (Section 3.1, situation I), while simulation II focuses on the performance of ECPSs under cyber attacks (Sections 3.2 and 3.3, situations II and III). Due to the fact that the IEEE database does not provide the capacity of the lines in these power grids, we refer to the similar concept of tolerance parameter (α) in Koç *et al.* (2014) to reflect the relationship between maximum capacity of a line and its base load. The authors showed that the system had a typical robustness when α ranged from 1.5 to 2.0, which means power flows in all the transmission

lines were within 50%–67% of the capacity. In this study, we conducted the simulation with $\alpha = 1.6$.

5.2 Simulation results

In simulation I, according to situation I, we randomly selected a transmission line $v = (i, j)$ as the initial triggering event ($k = 0$). The control strategy in situation I (Section 3.1) was applied at time $k = 1$, and the ECPS experienced the cascading failure propagation procedure (a)–(g). We focused on the number of the rest of nodes after cascading propagation. A comparison simulation was made to reflect the cascading failures in a simple physical power system in the same situation with the difference of $\boldsymbol{h} = \boldsymbol{0}$ during the whole process. Except the swing node and the line connected to the node, the remaining transmission lines in each system were numbered, respectively. Figs. 5–8 show the scale of cascading failures in the 9-, 14-, 30-, and 39-bus power systems and ECPSs, respectively. It can be verified that without cyber attacks, ECPSs have higher robustness than power systems owing to the real-time control strategy. Note that in Fig. 8, lines 36–45 are all connected to generators, so cutting off the line equals to cutting off the node. The current control strategy is more effective for generator nodes than load nodes reflected in the figure with a higher difference in δ. Figs. 5–7 illustrate the same conclusions as Fig. 8.

By analyzing the topology of each system, it can be seen that the 9- and 14-bus systems represent typical distribution grids, while the 30- and 39-bus systems represent different transmission grids. Our proposed framework has portability and can reflect the characteristics of electrical power flows at the same time. In Huang *et al.* (2015) and Zhao *et al.* (2015), power grids of Guangdong Province in China were used to design the framework of security operation by acquiring the topology of the Guangdong Communication Network and do the same work again when the situation was changed. The process is of heavy work and time-consuming. In Buldyrev *et al.* (2010) and Parshani *et al.* (2010), the modeling of ECPSs with the theory of complex network was too general to capture the characteristics of power systems.

In simulation II, ECPSs under cyber attacks were analyzed with the 39-bus system. Except the swing node 31 and the line $(31, 6)$ connected to the node, the remaining 45 transmission lines in the system were numbered from 1 to 45. According to

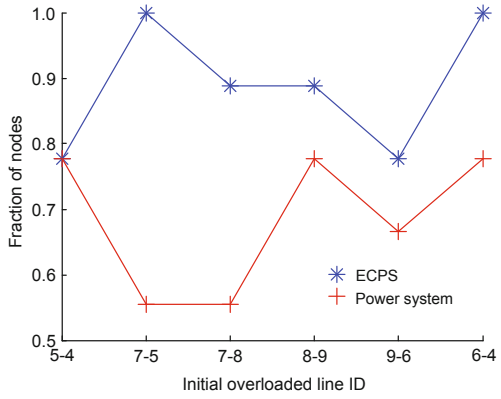

Fig. 5 The scale of cascading failures in the IEEE 9-bus system

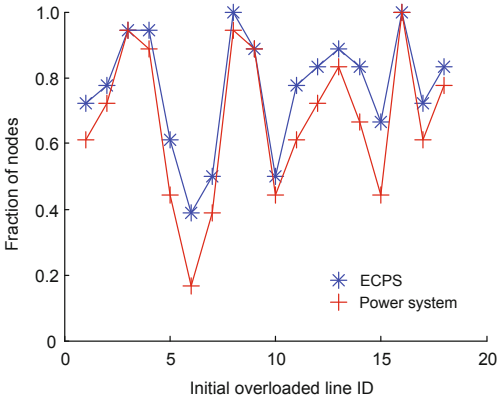

Fig. 6 The scale of cascading failures in the IEEE 14-bus system

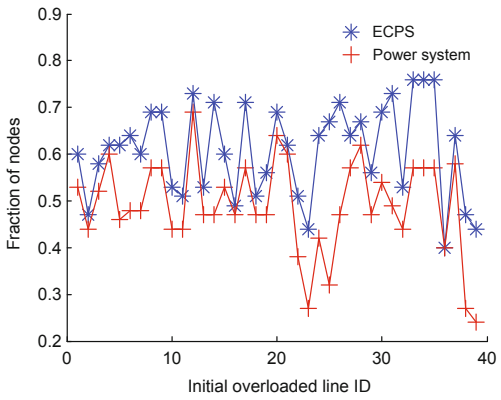

Fig. 7 The scale of cascading failures in the IEEE 30-bus system

situations II and III, we assumed that a DoS attack occurred at time $k = 1$ after an initial fault. As for false data injection attacks, we simulated the consequences of attacks occurring in region i ($i = 1, 2, 3$) with $h_i = 0.2p_i$. The influenced control strategies are as shown in Tables 2 and 4. The system still experienced the procedure (a)–(g). It is seen that ECPSs under DoS attacks may lead to a severe failure. As for replay attacks, the situation was influenced by the control policy at time w. The value of $\boldsymbol{h}[w]$ changed as the scale of the cascading failure varied, which was similar to situation III in which a system is under false data attacks, since both of the attacks aim at modifying the values of $\boldsymbol{h}$ by $\boldsymbol{h}[w]$ and $\boldsymbol{h}^{\text{active}}$. So, in Fig. 9, the performance of replay attacks is not displayed. Fig. 9 also shows the data of the system without attacks as reference (marked as stars).

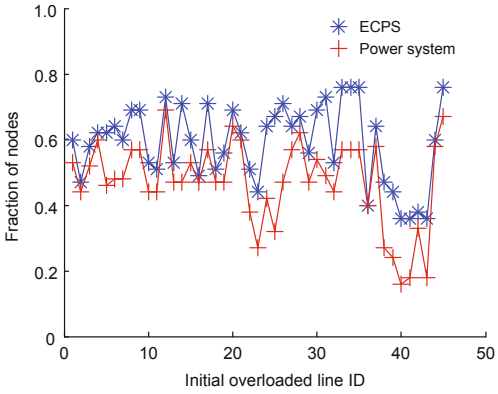

Fig. 8 The scale of cascading failures in the IEEE 39-bus system

6 Conclusions and future work

We have established a new framework for ECPSs where a communication network and its relationship are designed by the characteristics of a given power grid. In particular, we have characterized the interdependency of connected networks based on different types of information channels. Control strategies such as load shedding and relay protection, and attack scenarios have also been applied to the designed communication networks for analyzing cascading failure propagation. In the future, we will focus on fault detection and distributed control of ECPSs under cyber attacks based on the proposed framework for ECPSs. Also, there is need to investigate methods for detecting cyber attacks and redesigning control schemes to protect the whole system.

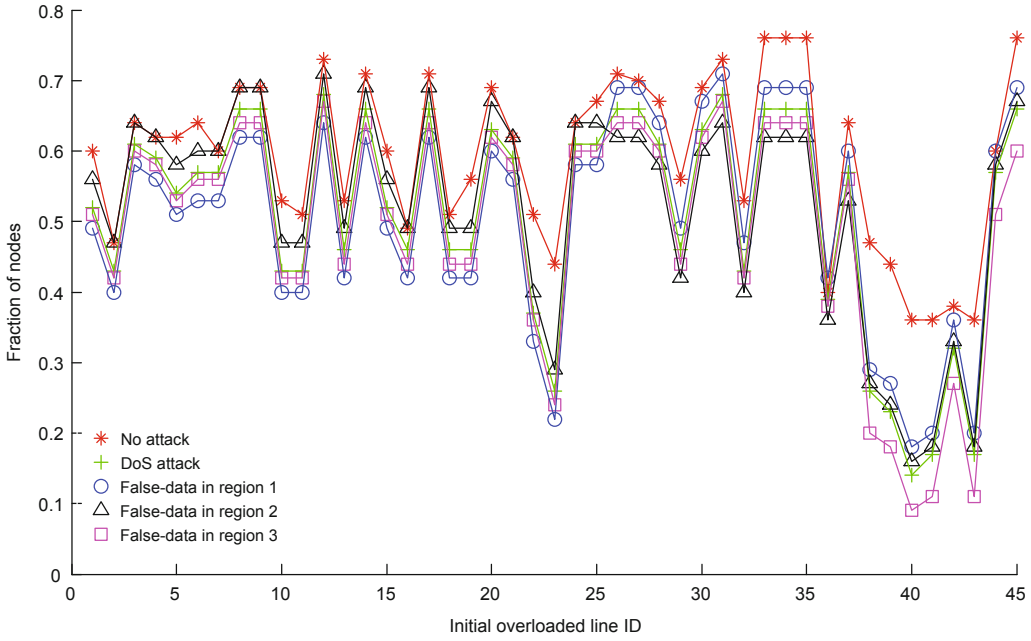

Fig. 9 The scale of cascading failures under attacks in the IEEE 39-bus system

References

Baldick, R., Chowdhury, B., Dobson, I., *et al.*, 2008. Initial review of methods for cascading failure analysis in electric power transmission systems. Proc. IEEE Power and Energy Society General Meeting, p.1-8. http://dx.doi.org/10.1109/PES.2008.4596430

Bao, Z.J., Cao, Y.J., Wang, G.Z., *et al.*, 2009. Analysis of cascading failure in electric grid based on power flow entropy. *Phys. Lett. A*, **373**(34):3032-3040. http://dx.doi.org/10.1016/j.physleta.2009.06.058

Bishop, M., 2002. Computer Security: Art and Science. Addison-Wesley Prefessional, USA.

Buldyrev, S.V., Parshani, R., Paul, G., *et al.*, 2010. Catastrophic cascade of failures in interdependent networks. *Nature*, **464**:1025-1028. http://dx.doi.org/10.1038/nature08932

Buldyrev, S.V., Shere, N.W., Cwilich, G.A., 2011. Interdependent networks with identical degrees of mutually dependent nodes. *Phys. Rev. E*, **83**:016112. http://dx.doi.org/10.1103/PhysRevE.83.016112

Chakrabarti, A., Manimaran, G., 2002. Internet infrastructure security: a taxonomy. *IEEE Netw.*, **16**(6):13-21. http://dx.doi.org/10.1109/MNET.2002.1081761

Chen, P.Y., Cheng, S.M., Chen, K.C., 2012. Smart attacks in smart grid communication networks. *IEEE Commun. Mag.*, **50**(8):24-29. http://dx.doi.org/10.1109/MCOM.2012.6257523

Dobson, I., Carreras, B.A., Lynch, V.E., *et al.*, 2001. An initial model for complex dynamics in electric power system blackouts. Proc. Hawaii Int. Conf. on System Sciences, p.1-9.

Gungor, V.C., Sahin, D., Kocak, T., *et al.*, 2011. Smart grid technologies: communication technologies and standards. *IEEE Trans. Ind. Inform.*, **7**(4):529-539. http://dx.doi.org/10.1109/TII.2011.2166794

Hu, Y., Ksherim, B., Cohen, R., *et al.*, 2011. Percolation in interdependent and interconnected networks: abrupt change from second- to first-order transitions. *Phys. Rev. E*, **84**:066116. http://dx.doi.org/10.1103/PhysRevE.84.066116

Huang, T.E., Sun, H.B., Guo, Q.L., *et al.*, 2015. Knowledge management and security early warning based on big simulation data in power grid operation. *Power Syst. Technol.*, **39**(11):3080-3087 (in Chinese).

Huang, X., Gao, J., Buldyrev, S.V., *et al.*, 2011. Robustness of interdependent networks under targeted attack. *Phys. Rev. E*, **83**:065101. http://dx.doi.org/10.1103/PhysRevE.83.065101

Koç, Y., Warnier, M., Mieghem, P.V., *et al.*, 2014. The impact of the topology on cascading failures in a power grid model. *Phys. A*, **402**:169-179. http://dx.doi.org/10.1016/j.physa.2014.01.056

Liu, Y., Ning, P., Reiter, M.K., 2011. False data injection attacks against state estimation in electric power grids. *ACM Trans. Inform. Syst. Secur.*, **14**(1):13.1-13.33. http://dx.doi.org/10.1145/1952982.1952995

Morris, R.G., Barthelemy, M., 2013. Interdependent networks: the fragility of control. *Sci. Reports*, **3**:2764.1-2764.5. http://dx.doi.org/10.1038/srep02764

Parandehgheibi, M., Modiano, E., Hay, D., 2014. Mitigating cascading failures in interdependent power grids and communication networks. Proc. IEEE Int. Conf. on Smart Grid Communications, p.242-247. http://dx.doi.org/10.1109/SmartGridComm.2014.7007653

Parshani, R., Buldyrev, S.V., Havlin, S., 2010. Interdependent networks: reducing the coupling strength leads to a change from a first to second order percolation transition. *Phys. Rev. Lett.*, **105**:048701. http://dx.doi.org/10.1103/PhysRevLett.105.048701

Pasqualetti, F., Dörfler, F., Bullo, F., 2013. Attack detection and identification in cyber-physical systems. *IEEE Trans. Autom. Contr.*, **58**(11):2715-2729. http://dx.doi.org/10.1109/TAC.2013.2266831

Schneider, C.M., Yazdani, N., Araújo, N.A.M., *et al.*, 2013. Towards designing robust coupled networks. *Sci. Reports*, **3**:1969.1-1969.7. http://dx.doi.org/10.1038/srep01969

Shao, J., Buldyrev, S.V., Havlin, S., *et al.*, 2011. Cascade of failures in coupled network systems with multiple support-dependence relations. *Phys. Rev. E*, **83**:036116. http://dx.doi.org/10.1103/PhysRevE.83.036116

Shin, D.H., Qian, D., Zhang, J., 2014. Cascading effects in interdependent networks. *IEEE Netw.*, **28**(4):82-87. http://dx.doi.org/10.1109/MNET.2014.6863136

Stott, B., Jardim, J., Alsac, O., 2009. DC power flow revisited. *IEEE Trans. Power Syst.*, **24**(3):1290-1300. http://dx.doi.org/10.1109/TPWRS.2009.2021235

Teixeira, A., Shames, I., Sandberg, H., *et al.*, 2015a. A secure control framework for resource-limited adversaries. *Automatica*, **51**:135-148. http://dx.doi.org/10.1016/j.automatica.2014.10.067

Teixeira, A., Sou, K.C., Sandberg, H., *et al.*, 2015b. Secure control systems: a quantitative risk management approach. *IEEE Contr. Syst.*, **35**(1):24-45. http://dx.doi.org/10.1109/MCS.2014.2364709

Wang, S.Z., 2012. Power System Control and Dispatching Automation (2nd Ed.). China Electric Power Press, China (in Chinese).

Wei, J., Kundur, D., Zourntos, T., *et al.*, 2014. A flocking-based paradigm for hierarchical cyber-physical smart grid modeling and control. *IEEE Trans. Smart Grid*, **5**(6):2687-2700. http://dx.doi.org/10.1109/TSG.2014.2341211

Yang, Q., Barria, J.A., Green, T.C., 2011. Communication infrastructures for distributed control of power distribution networks. *IEEE Trans. Ind. Inform.*, **7**(2):316-327. http://dx.doi.org/10.1109/TII.2011.2123903

Zhao, F., Sun, H.B., Huang, T.E., *et al.*, 2015. Design and engineering application of automatic discovery system for critical flowgates and security operation rules in power grids. *Autom. Elect. Power Syst.*, **39**(1):117-123 (in Chinese).