Yi-nan Wang, Zhi-yun Lin, Xiao Liang, Wen-yuan Xu, Qiang Yang, Gang-feng Yan, 2016. On modeling of electrical cyber-physical systems considering cyber security. *Frontiers of Information Technology & Electronic Engineering*, **17**(5):465-478. http: //dx.doi.org/10.1631/FITEE.1500446

On modeling of electrical cyber-physical systems considering cyber security

Key words: Cyber-physical systems, Cyber attacks, Cascading failure analysis, Smart grid

Corresponding author: Zhi-yun Lin
E-mail: linz@zju.edu.cn
ORCID: http://orcid.org/0000-0002-5523-4467

Motivation

- A smart grid is a modern electrical grid with improved reliability, efficiency, and safety. 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). 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.
- Therefore, we propose a proper framework for ECPSs to analyze possible cascading failures due to cyber attacks.

Method

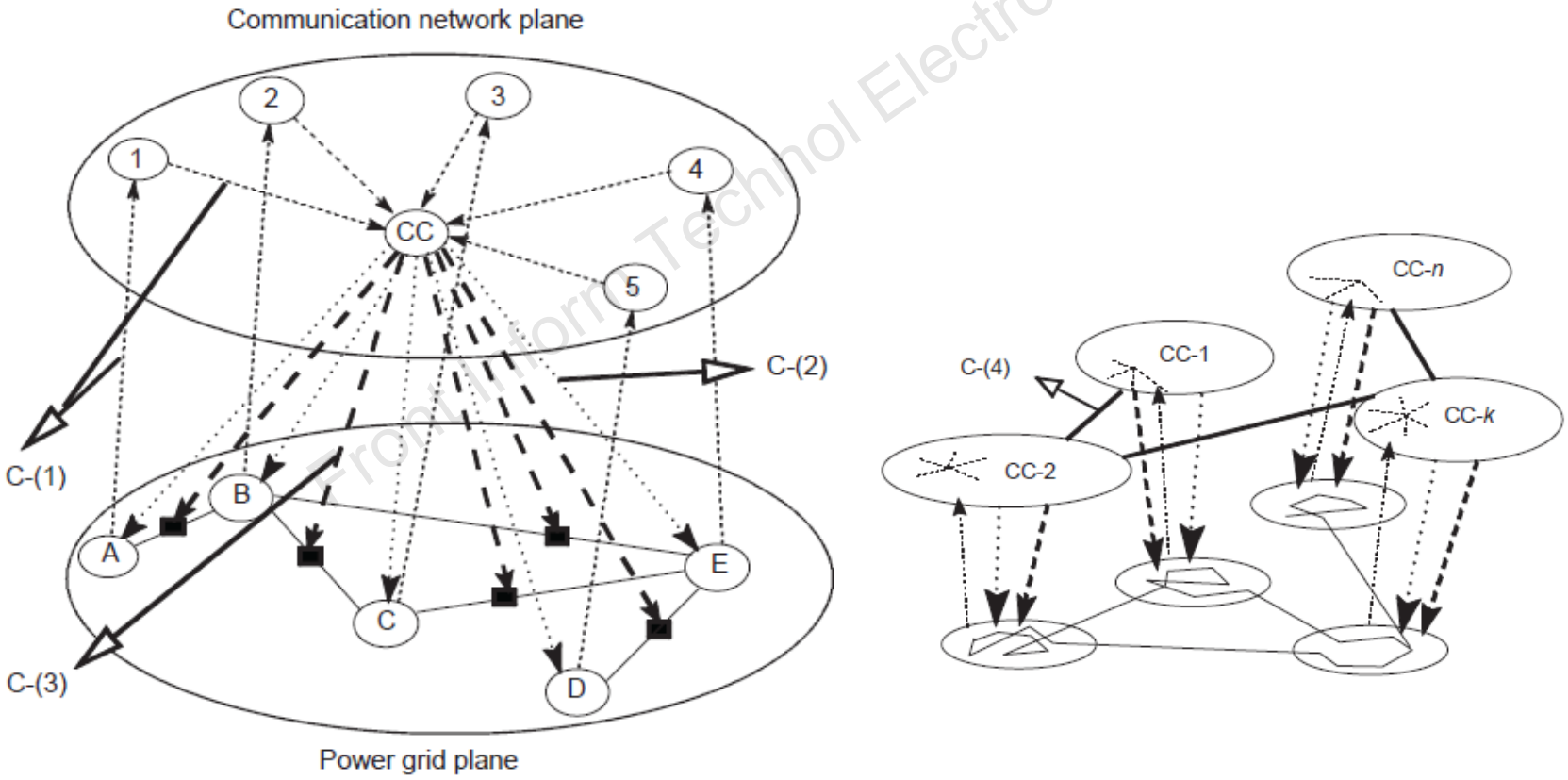
- First, we model the communication network associated with a power transmission grid, using a mesh network that considers the features of power transmission grids such as high-voltage levels, long-transmission distances, and equal importance of each node.

- Second, 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.

- Finally, 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 on this model against these attacks.

Major results

- Our proposed framework for ECPSs and its interdependent relationship



Major results (Con'd)

- Differences of modeling approaches on interdependent relationships are shown in Table 3.

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

Major results (Con'd)

The combination of ECPSs under different cyber attack scenarios at topological layer and control layer is described in Tables 5–7.

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

Table 7 An ECPS under the false data injection attack

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

Conclusions

- We have established a new framework for ECPSs where a communication network and its relationship is designed by the characteristics of a given power grid.

- This framework has portability, which can be used in any power system.

- We describe the relationship of 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.