Interdepedency modeling of cyber-physical systems using a weighted complex network approach

DOI:
10.1109/PTC.2017.7980807

Document Version
Accepted author manuscript

Link to publication record in Manchester Research Explorer

Citation for published version (APA):
Zhu, W., & Milanovic, J. V. (2017). Interdepedency modeling of cyber-physical systems using a weighted complex network approach. In *PowerTech, 2017 IEEE Manchester* https://doi.org/10.1109/PTC.2017.7980807

Published in:
PowerTech, 2017 IEEE Manchester

ACCEPTED VERSION OF THE PAPER

Interdepedency Modeling of Cyber-physical Systems Using a Weighted Complex Network Approach

Wentao Zhu, *Student Member IEEE*, and Jovica V. Milanović, *Fellow IEEE*,
School of Electrical and Electronic Engineering, The University of Manchester, Manchester, UK
wentao.zhu@manchester.ac.uk; milanovic@manchester.ac.uk

***Abstract*— This paper introduces a three-dimensional weighted Complex Network Theory (CNT) model to study the dependency and interdependency of cyber-physical systems (CPS) and to identify the most critical and vulnerable components within the coupled network. Based on CNT, the electric power buses within power system and communication routers and multiplexers within communication network are modelled as nodes, while the power lines and communication channels are modelled as edges. The intrinsic properties of electric power system (e.g. power flow) and the communication network (e.g. gross bitrate) are assigned as weights to each edge. A novel CNT-derived index, Vulnerability-weighted Node Degree (VWND), has been developed and applied to assess the dependency/importance of each physical/cyber node to its own and to the other system and such to help identify potentially weak areas of the system. The approach is illustrated on a 14-bus synthetic power distribution network with supporting Information and Communication Technologies (ICT).**

***Index Terms*-- Cyber-physical systems (CPS), Power distribution systems, Information and Communication Technologies (ICT), Complex networks, Critical Infrastructures Vulnerability**

I. Introduction

The study of the interactions between the cyber and physical systems requires a rethink of the overall approach to modeling and analysis of interconnected systems, i.e. System-of-systems [1]. Recent large-scale blackouts around the world have raised concerns about system vulnerability and emphasized importance of reinforcement of existing power and energy system infrastructure. These events suggested that ICT-dependent power systems are more vulnerable to cyber threats and terrorist attacks [2-4]. Cascading failures are recognized by the power system operators as the typical reasons of black-outs in power grids [5]. Due to the increased system complexity resulting from ever increasing penetration level of Distributed Energy Resources (DERs) and uncertain heterogeneous loads, power systems are required to be even more interlinked with Information and Communication Technologies (ICT) to facilitate monitoring and control of stochastic power generation and consumptions, as well as to maintain grid stability. This integration of ICT increases further the heterogeneity and complexity of this new system of systems. It has been pointed out in [6] that systems with high heterogeneity are particularly vulnerable to attacks and large-scale cascading failures could be triggered by disabling a single key node either within the power system or within the ICT network. ,

CPSs have been extensively researched during the past years, with ICT supported Smart Grid being one of the key case studies. An aspect-oriented approach to model the communication, fault, and timing issues of a smart grid, based on the application of distributed state estimation was proposed in [7], while a CPS reference model for smart grid, which is based on service-oriented computing paradigm, was presented in [8]. By studying the cyber-physical relationship and the impacts of an intentional attack on CPS on the proposed cyber-power testbed, an integration of Real Time Digital Simulator (RTDS) and Network Simulator 3 (NS3) was presented in [9]. A control system and communication system architecture of High Voltage Direct Current (HVDC) is proposed in [10] using a cyber-physical approach. The cyber security of the voltage control process of an active medium-voltage distribution system with a high level penetration of Renewable Energy Sources (RES) was discussed in [11] and a reliable and scalable communication network topology with multi-route information pathways to ensure critical data delivery within the smart electric power grid was proposed in [12]. Hierarchical multi-agent CPS for the modeling of smart grids, based on which the cyber-physical interactions are studied using flocking theory was introduced in [13], while the impact of cyberattack could have on a specific cyber-physical link, namely Automatic Generation Control (AGC) was investigated in [14].

Although this research into cyber-physical systems is very timely the risk assessment and vulnerability analysis in past approaches were purely based on the control (essentially ICT) side. It has to be pointed out however, that not only electric buses depend on cyber systems in order to maintain their normal operations, the cyber components also often receive power directly from electric power systems (EPS) to function, and an outage caused in the electrical network, even with moderate coupling, can cause severe malfunction of the ICT network [15] in spite of typically available back up supply. Therefore, an integrated framework to study the intra- and inter- dependency of CPS is highly needed.

This work was partly funded by the Research Councils UK, through the HubNet consortium (grant number: EP/I013636/1).

J. V. Milanović and W. Zhu are with the School of Electrical and Electronic Engineering, The University of Manchester, PO Box 88, Manchester, M60 1QD, UK. (email: milanovic@ manchester.ac.uk).

Agent-based modeling approaches (often integrated with complementary methods such as Monte Carlo simulations [16], Federated simulations [17], event-driven approaches [18], input-output inoperability model [19]) display a great flexibility in studying CPS. The requirement for parallel processing, however, makes them hard to be implemented in practice. Other methods including Bayesian Networks, Petri Networks and Fault Trees [20, 21] did not yet provide an accurate model to reveal the engineering structure of CPS and the results are sometimes too abstract to be understood. In fact, purely topological models of engineering systems always fail to capture the real behavior of such systems. The centrality distribution of electric power buses and power lines is very different from that developed purely based on its topological structure [22]. Power systems have been actively studied using weighted CNT theory, and a comprehensive analysis is presented in [23]. Nevertheless, there are few, if any, studies conducted on ICT network and CPS using weighted CNT-based methodologies.

In order to effectively address the issues discussed above, a weighted Complex Network Theory (CNT) model [24], developed from Graph Theory, has been introduced in this paper to study the non-trivial heterogeneous structure of the CPS. The paper for the first time introduces a three-dimensional weighted Complex Network model of CPS, which takes into account the electric power flow of the power system, and the gross bitrate of the cyber network. Based on the proposed model, a vulnerability index Vulnerability-weighted Node Degree (VWND) is introduced to assess the dependency and importance of each network component. The approach is illustrated on a 14-bus synthetic ICT-supported power distribution network. Compared to the binary model proposed in [25], the weighted model provides additional flexibility to study different engineering structures of the cyber-physical or interconnected systems.

II. Complex Network Modeling

A. Graphical Representation

It is evident that electric power systems (EPS) and ICT network have different patterns in sharing information, as shown in Fig. 1. The three-dimensional model endeavors to capture this asymmetric properties by modeling the connections with different engineering behaviors as bidirectional and unidirectional weighted edges respectively. As shown in Fig. 1, each layer represents a different intradependency type. Between the layers are the interdependency links based on the physical connection. In the case of a coupled power system and ICT infrastructure, the unidirectional power flows are presented in the upper layer, while the bidirectional exchanges of communication data are shown in the lower layer. Between these two layers, electric power is supplied from a power bus to a cyber component, while at the same time, the sensory data (state estimation and/or measurement data) are collected and sent from the power buses to control centers to allow necessary control command to be generated in the control centers and issued to the power buses. Systems' engineering properties, also known as electrical distances and cyber distances (e.g. power flow, gross bitrate), are unified and assigned as weights to corresponding edges.

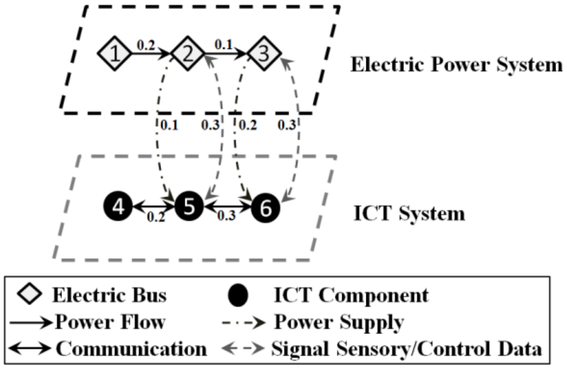

Fig. 1. Graph representation of CPS using weighted three-dimensional model

B. Weighted Adjacency Matrix

The two weighted adjacency matrices (W^e and W^c) of the electric layer and the ICT layer of the graphical model are introduced in (1) and (2).

$$W^e = \begin{bmatrix} w_{hj}^e & \cdots & w_{hm}^e \\ \vdots & \ddots & \vdots \\ w_{mj}^e & \cdots & w_{mm}^e \end{bmatrix} \tag{1}$$

$$W^c = \begin{bmatrix} w_{kl}^c & \cdots & w_{kn}^c \\ \vdots & \ddots & \vdots \\ w_{nl}^c & \cdots & w_{nn}^c \end{bmatrix} \tag{2}$$

They represent the relation between cyber and physical systems mathematically. The element w_{hj}^e represents the normalized electrical distance between node *h* and node *j*, while w_{kl}^c represents the normalized cyber distance between node *k* and node *l*. The weighted adjacency matrices for EPS and ICT systems are presented in (3) and (4).

$$W^e = \begin{bmatrix} 0 & 0.2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0.1 & 0 & 0.1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0.2 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{3}$$

$$W^c = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0.3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0.3 \\ 0 & 0 & 0 & 0 & 0.2 & 0 \\ 0 & 0.3 & 0 & 0.2 & 0 & 0.3 \\ 0 & 0 & 0.3 & 0 & 0.3 & 0 \end{bmatrix} \tag{4}$$

C. Efficiency and Vulnerability

Efficiency is first introduced in [26] to measure how efficiently the whole network exchanges information among nodes and edges.

$$\mathrm{E(G)} = \frac{1}{\mathrm{N(N-1)}} \sum_{i \neq j \in G} \frac{1}{d_{ij}} \tag{5}$$

where N is the number of nodes of the network G and d_{ij} is the shortest path between node *i* and *j*.

A pointwise measurement of a single component's (node or edge's) vulnerability index V_a can be defined as the global efficiency drop of the system after the removal of that component [27].

$$\mathrm{V(a)} = \frac{E(G) - E(G-a)}{E(G)} \tag{6}$$

The efficiency results for EPS and ICT systems of the example graph (Fig. 1) are presented in Table I.

TABLE I Example Graph Node Efficiency Results

Node	Base	1	2	3	4	5	6
E_e	0.0537	0.0407	0.0222	0.0185	0.0537	0.0352	0.0185
E_c	0.2679	0.2679	0.1190	0.1267	0.2222	0.0667	0.0933

D. Vulnerability-weighted Node Degree (VWND)

Node degree (ND) is the measure of a focal node's involvement within the network. In a binary bidirectional graph, it is quantified by the number of nodes the focal node is incident with, as defined in (7) [28].

$$D_i = \sum_{j}^{N} x_{ij} \tag{7}$$

where i is the focal node, j represents other nodes within the network, $\boldsymbol{N}$ is the total number of nodes within the network, and x_{ij} represents the connection between node i and j ('1' if there is a connection, '0' otherwise).

To better describe CPS engineering features, a complex-valued node degree (ND) is introduced to measure the criticality of each node. There are four types of connection within a CPS: *i) Type 1:* The power flow from an electrical node to another electrical node; *ii) Type 2:* The information flow from an ICT node to another ICT node; *iii) Type 3:* The electric energy supply from an electric node to an ICT node; *iv) Type 4:* The sensory data/control command from/to an electric node to/from an ICT node.

Each type of edge is weighted with a complex number as shown in Fig. 2. To be noted, a bidirectional ICT edge is regarded as an incoming edge and an outgoing link to each node.

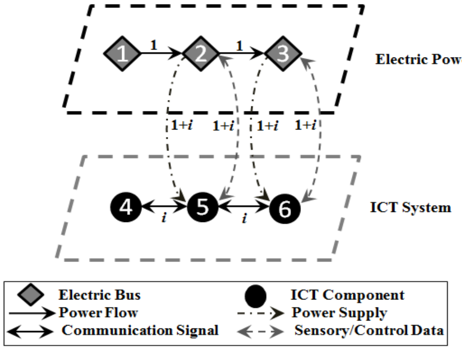

Fig. 2. Complex-valued edges

As shown in (8) and (9), the Complex-valued ND uses an in-degree D_i^{in} (number of incoming links) and an out-degree D_i^{out} (number of outgoing links) to measure node's dependency and importance respectively, and an electrical degree D_{ei} (real part) and an ICT degree D_{ci} (imaginary part) to categorize type of dependency/importance. The Complex-valued ND results for the example network shown in Fig. 2 are presented in Table II.

$$D_i^{in} = \sum_{j \in V} a_{ji} = D_{ei}^{in} + i \cdot D_{ci}^{in} \tag{8}$$

$$D_i^{out} = \sum_{j \in V} a_{ij} = D_{ei}^{out} + i \cdot D_{ci}^{out} \tag{9}$$

TABLE II Complex-valued Node Degree

Node	1	2	3	4	5	6
D_i^{in}	0	2+i	2+i	i	2+4i	2+3i
D_i^{out}	1	3+2i	2+2i	i	1+3i	1+2i

Weighted network studies extended the definition of ND to represent node's strength S_i [29,30].

$$S_i = \sum_{j}^{M} F_{ij} \tag{10}$$

where i is the focal node, j represents other nodes within the network, M is the total number of links node i has, and F_{ij} represents the strength of the connection between node i and j.

The Vulnerability-weighted Node Degree (VWND) introduced in this paper went along the same concept with the vulnerability of each edge computed on the basis of the weighted network. Similarly to Complex-valued ND, the VWND of each node is composed of four components, namely electrical in-degree D_e^{in}, electrical out-degree D_e^{out}, ICT in-degree D_c^{in} and ICT out-degree D_c^{out}. The vulnerability-weighted in-degrees for an electric node i and an ICT node k, which represent their dependencies from both electric and ICT systems, are calculated by (11) and (12), while the vulnerability-weighted out-degrees, which represent their importance to both electric and ICT systems, are calculated by (13) and (14).

$$\begin{aligned} D_i^{in} &= D_{ei}^{in} + i \cdot D_{ci}^{in} \\ &= \sum_{j \in V_e, i \in V_e, j \neq i} a_{ji}^{e} \cdot V_{e,ji} + i \cdot \sum_{k \in V_c, i \in V_e, k \neq i} a_{ki}^{c} \cdot V_{c,ki} \end{aligned} \tag{11}$$

$$\begin{aligned} D_k^{in} &= D_{ek}^{in} + i \cdot D_{ck}^{in} \\ &= \sum_{j \in V_e, k \in V_c, j \neq k} a_{jk}^{e} \cdot V_{e,jk} \\ &+ i \cdot \Big(\sum_{j \in V_e, k \in V_c, j \neq k} a_{jk}^{c} \cdot V_{c,jk} + \sum_{l \in V_c, k \in V_c, l \neq k} a_{lk}^{c} \cdot V_{c,lk} \Big) \end{aligned} \tag{12}$$

$$\begin{aligned} D_i^{out} &= D_{ei}^{out} + i \cdot D_{ci}^{out} \\ &= \sum_{i \in V_e, j \in V_e, i \neq j} a_{ij}^{e} \cdot V_{e,ij} + \sum_{i \in V_e, k \in V_c, i \neq k} a_{ik}^{e} \cdot V_{e,ik} \\ &+ i \cdot \sum_{i \in V_e, k \in V_c, i \neq k} a_{ik}^{c} \cdot V_{c,ik} \end{aligned} \tag{13}$$

$$D_k^{out} = D_{ek}^{out} + i \cdot D_{ck}^{out} = i \cdot \Big(\sum_{k\in V_c, j\in V_e, k\neq j} a_{kj}^{c} \cdot V_{c,kj} + \sum_{k\in V_c, l\in V_c, k\neq l} a_{kl}^{c} \cdot V_{c,kl} \Big) \qquad (14)$$

where a_{ij}^{e} and a_{kl}^{c} are the entries of complex-valued adjacency matrices for electric layer and ICT layer, and $V_{e,ij}$ and $V_{c,kl}$ are the electrical and cyber vulnerabilities associated with each edge, as calculated in (6). Table III presents the VWND results for the example network shown in Fig. 1.

TABLE III VULERABILITY-WEIGHTED NODE DEGREE

Node	1	2	3	4	5	6
D_i^{in}	0	0.8+0.4i	0.7+0.3i	0.4i	0.5+1.4i	0.7+1.2i
D_i^{out}	0.5	0.9+0.5i	0.7+0.7i	0.4i	0.4+1.2i	0.3+0.8i

III. TEST SYSTEM AND RESULTS

A. Test System

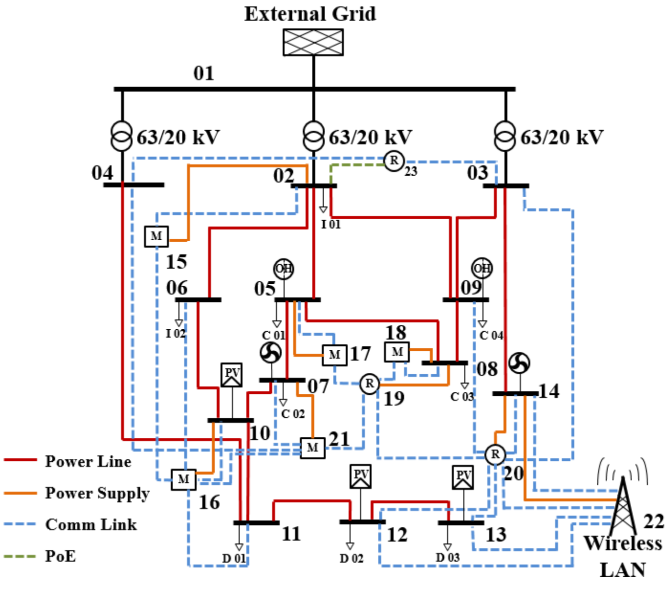

Fig. 3. Test system: 14-bus micro-grid with ICT

The test system is a 14-bus synthetic distribution system with supporting ICT network. The power system within the coupled network contains 14 buses, 17 power lines, 7 distributed generators (Photovoltaic Generators, Wind Generators, Fuel Cells), 9 loads (domestic, commercial and industrial modelled using corresponding daily loading curves) and 3 HV/MV transformers (see Fig. 3). The electricity generation and consumption vary with time during the year, creating a time-dependent power flow for the electric part of the interconnected system. The subsequent case study is based on the annual maximum loading (6470th hour of the year) of the power distribution network. The supporting ICT system is comprised of information repeaters/aggregators and distributed information processing centers which are represented by 3 routers and 5 multiplexers for simplicity. There are several information technologies to enable the effective and efficient monitoring and controlling of power system, which includes LAN-Giga Ethernet, Wireless LAN, Ethernet and Fiber Optics. Specifically for the communication link 2-23, the power and communication signal share the same transmission channel which is known as Power over Ethernet (PoE). The state estimation data are collected from the EPS and sent to ICT system, after being processed and analyzed at the ICT site, control signals are issued and sent back to enable certain functions of EPS. The ICT site runs as a small-scale Supervisory Control and Data Acquisition (SCADA) system, which is equipped with sufficient amount of capacity and data transmission speed to allow its smooth and constant cyber functions.

B. Three-dimensional CPS Model

The three-dimensional CPS model for the test system is presented in Fig. 4. Power system buses and ICT routers and multiplexers are modelled as red and blue nodes in the upper and lower layers respectively. Power system's unidirectional power flow and ICT's full-duplex transmission of information are modelled as unidirectional edges and bidirectional edges respectively. Between power and ICT layers, red dash dot lines, there are power supplies from power system to ICT network, while blue dashed lines represent the simultaneous collection of sensor data from sensors and transmission of control data between ICT and actuators.

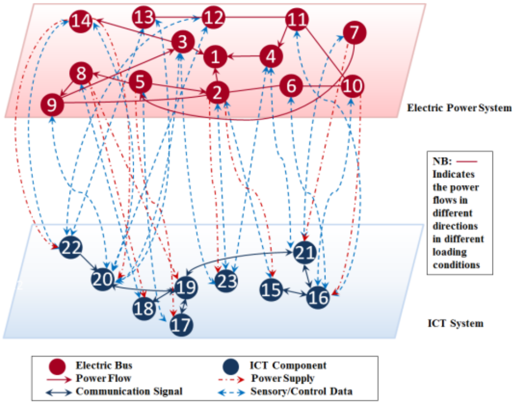

Fig. 4. Three-dimensional CPS model for test system

C. Electrical Shortest Path and Cyber Shortest Path

The electrical shortest path refers to the electrical path that possesses the maximum likelihood of power flow which is equivalent to the least reactance path in power systems [31], as illustrated in (15).

$$P_{pq} = \frac{v_p v_q}{x_{pq}} \sin \alpha_{pq} \qquad (15)$$

Theoretically the power flowing through any network is dependent on the nodal voltages and line parameters. Assuming lossless power lines within the EPS and regulated (very close to rated) nodal voltages v_p and v_q, and small phase angle difference α_{pq} (typical for short and reasonably lightly loaded lines) the active power flow $\mathrm{P_{pq}}$ is inversely proportional to line reactance $\mathrm{x_{pq}}$, i.e. $\mathrm{P_{pq}} \propto \frac{1}{\mathrm{X_{pq}}}$, or $\frac{1}{\mathrm{P_{pq}}} \propto \mathrm{X_{pq}}$. Therefore, the shortest electrical path is the electrical path with minimum sum of $\frac{1}{\mathrm{P_{pq}}}$.

On the ICT network side, power grid's performance relies heavily on not only optimal control algorithms, but also communication network requirements to fulfil its smart functionalities, such as voltage angle per bit and maximum power factor per bit [32]. Therefore, the communication speed, i.e. bit transmission time, is also a critical criterion to be considered for the supporting ICT network. The relationship between bit transfer time and gross bitrate is presented in (16).

$$R_b = \frac{n}{T} = \frac{n}{nT_b} = \frac{1}{T_b} \qquad (16)$$

where n is the number of bits per symbol, T is the symbol duration and T_b is the bit transmission time.

It can be easily found out from (16) that $\mathrm{T_b} \propto \frac{1}{\mathrm{R_b}}$. As a result, the shortest cyber path, representing the fastest communication channel between a pair of ICT nodes k and l has the minimum sum of $\frac{1}{\mathrm{R_b}}$.

The cyber and physical networks parameters are normalized using Gaussian Membership function [33] with the largest value in each corresponding system selected as the base value. Only a small subset of results are presented in Table IV and Table V due to space limitation.

TABLE IV ICT PARAMETERS AND CYBER DISTANCE

ICT Connections		Technology	Gross bitrate (bps)	Normalized $\frac{1}{\mathrm{R_b}}$
23	2	LAN-Giga [34]	36G	0.2148
15	2	Ethernet [35]	90M	0.6370
15	16	Fiber Optics[35]	9G	0.2842

TABLE V EPS PARAMETERS AND ELECTRICAL DISTANCE

Power Line		Power Flow (MW)	Normalized $\frac{1}{\mathrm{P_{pq}}}$
2	1	3.3	0.2105
7	5	1.4	0.4064
13	12	1	0.6754

D. Vulnerability-weighted Node Degree (VWND)Results

Based on the electrical shortest path and cyber shortest path, the VWND of coupled system (electric edges weighted with power flow values and cyber edges weighted with gross bitrate values) is calculated and presented in Fig. 5 and Fig. 6. Fig. 5 displays nodal electrical and ICT in-degree (physical and cyber dependency). It shows that each system node (except for external grid node 1) has dependencies on both systems. Electric system has a relatively high intra-dependency, however, cyber system has an overall higher dependency, which makes it more vulnerable to physical and cyberattacks. Especially, the normal function of nodes 16 and 20 are most dependent on both electric and ICT systems. Fig. 6 presents nodal electrical and ICT out-degree (physical and cyber importance). It shows that all EPS system nodes (except for external grid node 1) influence the cyber system. Vertices 16 and 20 are important for both systems. To be noted, central router 19 has the highest cyber importance and a relatively high cyber dependence, therefore it is the most critical ICT node although it does not control any electric bus directly. Fig. 7 and Fig. 8 illustrate the dependency and importance of most critical electric buses 3 and 8, and ICT routers 19 and 20. Similar diagrams can be produced for any EPS or ICT node.

In general, ICT system displays a star topology with several key components being more vulnerable, as well as critical for both cyber and physical systems. Therefore, prevention of failure and countermeasures should be designed carefully for these nodes.

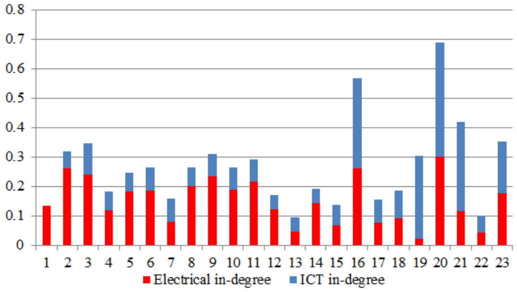

Fig. 5. Nodal electrical and ICT in-degree

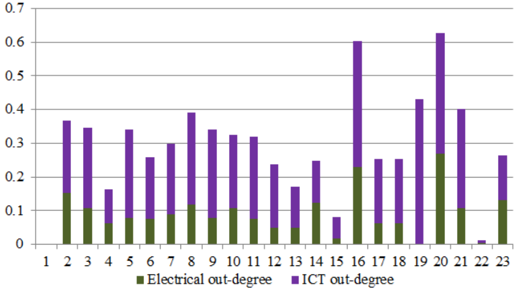

Fig. 6. Nodal electrical and ICT out-degree

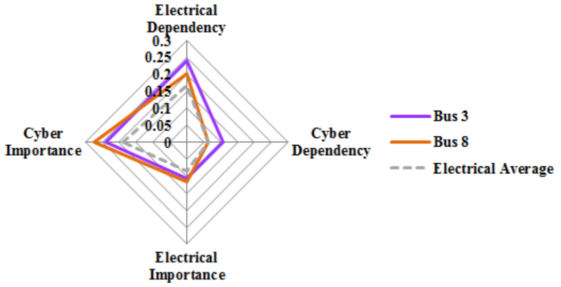

Fig. 7. Comparison of dependency and importance – electrical buses 3 and 8

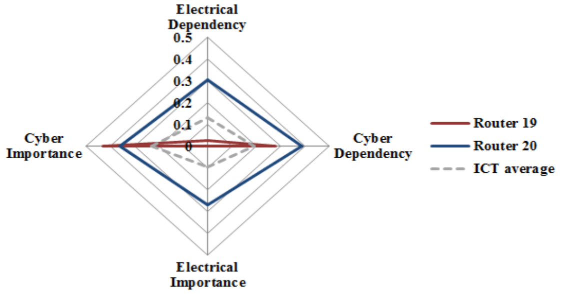

Fig. 8. Comparison of dependency and importance – ICT routers 19 and 20

IV. CONCLUSIONS

By implementing Complex Network Theory, this paper proposes a novel design approach for weighted modeling of CPS and introduces a weighted three-dimensional complex-network model, which incorporates the heterogeneous system characteristics. In this way, different engineering structures of CPS can be studied without any modification to the topological model.

Based on the presented CNT-based model, the paper provides the results of extensive simulation study, revealing the vulnerability of different engineering systems and the critical components which could initiate a cascading failure due to the interdependencies between systems. It provides a starting point to analyze the 'Smart Grid' as an integrated system, and enables the cyber security and risk assessment, and thereafter risk management and defense strategies to be developed.

The illustrative results presented in the paper show that a cyber-focused attack can initiate much larger-scale cascading failure effects to the CPS compared to the one caused by the failure of a central electric bus, and therefore the central cyber components should be carefully protected from intentional attacks. The macroscopic-scale relations among different infrastructure systems established in this paper can be used as a generic framework for further in-depth (focus) analysis accounting for associated system uncertainties.

References

[1] A. Gorod, B. Sauser, and J. Boardman, "System-of-Systems Engineering Management: A Review of Modern History and a Path Forward," *IEEE Systems Journal*, vol. 2, pp. 484-499, 2008.

[2] E. F. Halpin, *Cyberwar, netwar and the revolution in military affairs.* New York: Palgrave Macmillan, 2006.

[3] U.S. Dept. Homeland Security (2015). ICS-CERT Monitor [Online]. Available: https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Nov-Dec2015_S508C.pdf

[4] N. Falliere, L. O. Murchu, and E. Chien, "W32.stuxnet dossier," Symantec Corp., Cupertino, CA, Feb. 2011.

[5] Y. Koc, M. Warnier, R. Kooij, and F. Brazier, "Structural Vulnerability Assessment of Electric Power Grids," *2014 IEEE 11th International Conference on Networking, Sensing and Control (ICNSC),* pp. 386-391, 2014.

[6] A. E. Motter and Y. C. Lai, "Cascade-based attacks on complex networks," *Physical Review E,* vol. 66, Dec 2002.

[7] I. Akkaya, Y. Liu, and E. A. Lee, "Modeling and Simulation of Network Aspects for Distributed Cyber-Physical Energy Systems," *Cyber Physical Systems Approach to Smart Electric Power Grid,* pp. 1-23, 2015.

[8] M. U. Tariq, S. Grijalva, and M. Wolf, "A Service-Oriented, Cyber-Physical Reference Model for Smart Grid," *Cyber Physical Systems Approach to Smart Electric Power Grid,* pp. 25-42, 2015.

[9] C. B. Vellaithurai, S. S. Biswas, R. Liu, and A. Srivastava, "Real Time Modeling and Simulation of Cyber-Power System," *Cyber Physical Systems Approach to Smart Electric Power Grid,* pp. 43-74, 2015.

[10] L. Nordstrom and D. Babazadeh, "Cyber Physical Approach to HVDC Grid Control," *Cyber Physical Systems Approach to Smart Electric Power Grid,* pp. 75-101, 2015.

[11] G. Dondossola and R. Terruggia, "Cyber Security of Smart Grid Communications: Risk Analysis and Experimental Testing," *Cyber Physical Systems Approach to Smart Electric Power Grid,* pp. 169-193, 2015.

[12] C. Zimmer and F. Mueller, "Reliable and Scalable Communication for the Power Grid," *Cyber Physical Systems Approach to Smart Electric Power Grid,* pp. 195-217, 2015.

[13] J. Wei and D. Kundur, "Biologically Inspired Hierarchical Cyber-Physical Multi-agent Distributed Control Framework for Sustainable Smart Grids," in *Cyber Physical Systems Approach to Smart Electric Power Grid,* K. S. Khaitan, D. J. McCalley, and C. C. Liu, Eds. Berlin, Germany: Springer, 2015, pp. 219-259.

[14] M. Vrakopoulou, P. M. Esfahani, K. Margellos, J. Lygeros, and G. Andersson, "Cyber-Attacks in the Automatic Generation Control," *Cyber Physical Systems Approach to Smart Electric Power Grid,* pp. 303-328, 2015.

[15] V. Rosato, L. Issacharoff, F. Tiriticco, S. Meloni, S. De Porcellinis, and R. Setola, "Modelling interdependent infrastructures using interacting dynamical models," *Int. J. Critical Infrastructures,* vol. 4, pp. 63-79, 2008.

[16] Y. Y. Haimes, B. M. Horowitz, J. H. Lambert, J. R. Santos, C. Lian, and K. G. Crowther, "Inoperability Input-Output Model for Interdependent Infrastructure Sectors. I: Theory and Methodology," *Journal of Infrastructure Systems,* vol. 11, pp. 67-79, 2005.

[17] E. Casalicchio, E. Galli, and S. Tucci, "Federated Agent-based Modeling and Simulation Approach to Study Interdependencies in IT Critical Infrastructures," in *Distributed Simulation and Real-Time Applications, 2007. DS-RT 2007. 11th IEEE International Symposium*, 2007, pp. 182-189.

[18] I. Eusgeld, W. Kröger, G. Sansavini, M. Schläpfer, and E. Zio, "The role of network theory and object-oriented modeling within a framework for the vulnerability analysis of critical infrastructures," *Reliability Engineering & System Safety,* vol. 94, pp. 954-963, 2009.

[19] Y. Y. Haimes and P. Jiang, "Leontief-Based Model of Risk in Complex Interconnected Infrastructures," *Journal of Infrastructure Systems,* vol. 7, pp. 1-12, 2001.

[20] D. W. Benbow and H. W. Broome, *The certified reliability engineer handbook*. Milwaukee, WIS.: ASQ Quality Press, 2009.

[21] E. Kyriakides and M. Polycarpou, Eds., *Intelligent monitoring, control, and security of critical infrastructure systems*. Berlin, Germany: Springer, 2014.

[22] P. Hines and S. Blumsack, "A Centrality Measure for Electrical Networks," in *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual*, 2008, pp. 185-185.

[23] G. A. Pagani and M. Aiello, "The Power Grid as a complex network: A survey," *Physica a-Statistical Mechanics and Its Applications,* vol. 392, pp. 2688-2700, June 2013.

[24] S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, and D. U. Hwang, "Complex networks: Structure and dynamics," *Physics Reports-Review Section of Physics Letters,* vol. 424, pp. 175-308, Feb. 2006.

[25] J. V. Milanović and W. Zhu, "Modelling of Interconnected Critical Infrastructure Systems Using Complex Network Theory," *IEEE Trans. Smart Grid*, in press.

[26] V. Latora and M. Marchiori, "Efficient behavior of small-world networks," *Physical Review Letters,* vol. 87, Nov 2001.

[27] V. Gol'dshtein, G. A. Koganov, and G. I. Surdutovich, Vulnerability and Hierarchy of Complex Networks. arXiv:cond-mat/0409298, 2004.

[28] L. C. Freeman, "Centrality in Social Networks Conceptual Clarification," *Social Networks,* vol. 1, pp. 215-239, 1979.

[29] A. Barrat, M. Barthelemy, R. Pastor-Satorras, and A. Vespignani, "The architecture of complex weighted networks," *Proceedings of the National Academy of Sciences of the United States of America,* vol. 101, pp. 3747-3752, Mar. 2004.

[30] M. E. J. Newman, "Analysis of weighted networks," *Physical Review E,* vol. 70, 2004.

[31] A. Dwivedi, X. H. Yu, and P. Sokolowski, "Identifying Vulnerable Lines in a Power Network using Complex Network Theory," *2009 IEEE International Symposium on Industrial Electronics (ISIE)*, pp. 18-23, 2009.

[32] F. B. Stephen, "What is Smart Grid Communication?," in *Smart Grid: Communication-Enabled Intelligence for the Electric Power Grid*, ed: Wiley-IEEE Press, 2013, pp. 576.

[33] Ch. S. Reddy and K. Raju, "An Improved Fuzzy Approach for COCOMO's Effort Estimation using Gaussian Membership Function, " *Journal of Software*, vol. 4, pp. 452-459, 2009.

[34] P. Shivam, P. Wyckoff, and D. Panda, "EMP: Zero-Copy OS-Bypass NIC-Driven Gigabit Ethernet Message Passing," in *Supercomputing, ACM/IEEE 2001 Conference*, 2001, pp. 49-49.

[35] P. Kyoung Shin and R. V. Kenyon, "Effects of network characteristics on human performance in a collaborative virtual environment," in *IEEE Virtual Reality*, 1999, pp. 104-111.